# Independent Auditor's Report

An Independent Auditor's Report on
Controls Relevant to HIPAA

Hashforest Technology LLC

June 5, 2026

AUDIT AND ATTESTATION BY

PRESCIENT
SECURITY

Prescient Security LLC.
1900 Church Street, Suite 300
Nashville, TN, 37203

www.prescientsecurity.com
+1 646 209 7319

# Table of Contents

# Independent Auditor's Report

To: Hashforest Technology LLC

## Summary

We have performed the procedures enumerated below on controls relevant to HIPAA as of June 5, 2026. Hashforest Technology LLC is responsible for the controls relevant to HIPAA.

Hashforest Technology LLC has agreed to and acknowledged that the procedures performed are appropriate to meet the intended purpose of assessing the company's compliance with HIPAA as of June 5, 2026. This report may not be suitable for any other purpose. The procedures performed may not address all the items of interest to a user of this report and may not meet the needs of all users of this report and, as such, users are responsible for determining whether the procedures performed are appropriate for their purposes.

We were engaged by Hashforest Technology LLC to perform this engagement and conducted our engagement in accordance with audit standards established by ISO 19011. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

The scope of this engagement is limited to the systems and processes used by Hashforest Technology LLC.

We are required to be independent of Hashforest Technology LLC and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements related to our agreed-upon procedures engagement.

This report is intended solely for the information and use of Hashforest Technology LLC, user entities of Hashforest Technology LLC's system as of June 5, 2026, business partners of Hashforest Technology LLC subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the organization.
- How the organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- The risks that may threaten the achievement of the organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Signed by:
Prescient Security
CCD00943BAE0483...

Prescient Security
June 29, 2026

# System Scope and Purpose

## Company Overview and Types of Products and Services Provided

Hashforest Technology LLC is a technology company based in California, United States, operating the Phala Cloud platform. The company specializes in providing secure and confidential computing infrastructure for businesses and developers, leveraging Trusted Execution Environment (TEE) technology to ensure privacy-preserving computation. Hashforest Technology LLC acts as the processor of personal data under applicable data protection laws and maintains strict controls and infrastructure to enforce data isolation and limit access to customer data. The organization's operations are governed by the laws of the State of California. Phala Cloud, operated by Hashforest Technology LLC, offers a cloud platform designed for building and deploying AI agents and Web3 applications. The platform provides scalable cloud computing solutions with the trust and privacy of blockchain technology, serving clients who require privacy-preserving computation for sensitive workloads. Data processed on Phala Cloud is encrypted and secured using TEE technology, and user interactions with large language model applications are kept confidential, with no access or retention of user prompts or inputs by the platform. The company's services include infrastructure hosting, product analytics, payment processing, customer relationship management, and marketing and email services, supporting a wide range of business and developer needs in regulated and privacy-focused domains.

## The Principal Service Commitments and System Requirements

Hashforest Technology LLC designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Hashforest Technology LLC makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Hashforest Technology LLC has established for the services. The system services are subject to the Security commitments established internally for its services. Hashforest Technology LLC's commitments to users are communicated through Service Level Agreements, Master Services Agreements, Statements of Work, Work Orders, Online Privacy Policy and Terms of Use.

### Security commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Regular vulnerability scans over the system and network, and penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal procedures.

# The Components of the System Used to Provide the Services

## Infrastructure & Network Architecture

| Application/ System | Process/ Transaction | Purchased or Developed | Platform and Operating System | Data Type |
|---|---|---|---|---|
| OVH | Cloud Infrastructure Provider | Purchased | IAAS | Encrypted workload data is stored |
| Cloudflare | CDN, DDoS protection, WAF, DNS | Purchased | SAAS | Network traffic metadata |
| GitHub | Source control, CI/CD pipelines | Purchased | SAAS | Source code, configuration |
| Drata | Compliance automation and monitoring | Purchased | SAAS | Audit evidence, policy records |
| Google Workspace | Email, document collaboration | Purchased | SAAS | PII, business communications |
| Slack | Internal communication | Purchased | SAAS | Employee messages |
| Zendesk | Customer support and helpdesk | Purchased | SAAS | Customer contact and ticket data |

## People

People Operations functions are managed jointly by the Operations and Security teams. The same personnel handle onboarding/offboarding, security training, and compliance documentation following standardized procedures.

## Security Processes and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by the executive team and COO. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment

- Data Retention
- Vendor Management

## Physical Security

Hashforest Technology LLC Phala Cloud's core production workloads are deployed on self-managed servers located in enterprise-grade data centers, supplemented by leased GPU resources (e.g., NVIDIA H200) from infrastructure providers such as OVH. The physical and environmental security protections are the responsibility of Subservice providers. Hashforest Technology LLC reviews the attestation reports and performs a risk analysis of OVH.

## Logical Access

The Logical Access section of Hashforest Technology LLC's System Access Control Policy outlines stringent controls for user authentication and authorization. Access to systems and applications is granted based on role-based access control (RBAC) and the principle of least privilege, ensuring that users only have access necessary for their job functions. The process for granting, modifying, and revoking access involves formal requests through a ticketing system, identity verification, and approval by the Security Officer. Access reviews are conducted regularly to maintain proper authorizations, and any discrepancies are addressed promptly. Unique user identification is enforced through strong password policies and the prohibition of shared accounts. Multi-factor authentication (MFA) is mandated for administrative access. Additionally, automated logoff mechanisms are in place to secure unattended systems. Access management is supported by a comprehensive directory of user accounts, which includes details such as account holder names, usernames, and access dates. Accounts are reviewed quarterly and deactivated after 45 days of inactivity. The policy also includes specific procedures for employee termination to ensure timely revocation of access rights. IT Support is responsible for provisioning access to the system based on the employee's role and performing a background check. All new employees are required to review Hashforest Technology LLC's Security, Privacy, and Acceptable Use Policies and complete mandatory security awareness training within three business days of onboarding.

## Computer Operations - Backups

The Backup Policy of Hashforest Technology LLC ensures the protection of data confidentiality, integrity, and availability through comprehensive backup procedures. Complete backups are performed to safeguard data against catastrophic loss, with all business data stored or replicated in a company-controlled repository. Backups are conducted automatically and encrypted similarly to live production data, with data stored in a separate region within the same country to ensure durability. The policy mandates that data retention periods comply with regulatory and contractual requirements, with security documentation and audit trails retained for a minimum of seven years. Access to backup data is controlled, and restoration procedures are in place to recover data in the event of a disaster. Additionally, Hashforest Technology LLC maintains multiple copies of data in diverse locations to ensure continuity and provide restoration capabilities after disruptive events.

## Computer Operations - Availability

Hashforest Technology LLC ensures system uptime and availability through comprehensive measures including redundancy and failover mechanisms, disaster recovery, and business continuity strategies. The Business Continuity Plan mandates the definition and documentation of backup and recovery processes for systems and data, with annual simulations and tests to measure metrics and identify recovery enhancements. Security controls are maintained at both primary and alternate sites during all continuity activities and disruptions. Preventative maintenance and monitoring of critical systems are overseen by the DevOps team, which is responsible for applications, web services, platforms, and supporting infrastructure in the Cloud. Incident response to availability threats is managed by the Security team, which assesses and responds to cybersecurity incidents as per the Incident Response policy. Additionally, the policy outlines the roles and responsibilities of various response teams, ensuring a structured approach to maintaining system availability and recovering from disruptions.

### Change Management

Hashforest Technology LLC's Change Management Policy outlines comprehensive procedures for requesting, approving, and implementing changes to system components, including infrastructure, code, and networking changes. All changes must be documented with a detailed description and security impact assessment. Testing is mandatory to ensure changes do not compromise system security, and formal approval is required before any work begins. Changes are implemented at times least disruptive to business processes, with pre-production environments strictly segregated from production environments. Extensive testing, including usability, security, and user-friendliness, is conducted in separate test environments. The policy mandates a rollback strategy and maintains audit logs for all updates to operational program libraries. Version control is enforced through a configuration control system, retaining previous software versions for contingency. Change tracking and auditing are supported by a configuration status accounting function, ensuring all changes are recorded and reported. Segregation of duties is maintained, with changes deployed to production only by authorized personnel with escalated privileges, and utility programs access restricted to a minimum number of authorized users.

### Data Communications

Hashforest Technology LLC has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Hashforest Technology LLC application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints. The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware. Hashforest Technology LLC uses an external service provider to perform periodic security scans. Vulnerability scans are performed on a monthly cycle and penetration testing is performed on an annual basis.

## Data

Hashforest Technology LLC's Data Classification Policy outlines the categorization of data into four levels: Restricted, Confidential, Internal Use, and Public. Restricted data includes highly sensitive information requiring external legal or contractual protection, while confidential data is sensitive information protected internally. Internal Use data encompasses non-sensitive information that must be protected from unauthorized access, and Public data is freely shareable with no risk to business operations. Access to Restricted and Confidential data is limited to authorized individuals with a legitimate need-to-know, and encryption is required for transmission and storage. Internal Use data is protected by reasonable security controls, and Public data requires minimal protection. Data retention and destruction policies mandate that data be destroyed when no longer needed, following specific company procedures. The policy ensures compliance with regulatory and contractual data protection requirements, applying stringent security measures throughout the data lifecycle.

# Procedures Performed and Findings

## Types of Tests Generally Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the design and implementation of the controls detailed in the matrices that follow:

| Test Types | Description of Tests |
|---|---|
| Inquiry | Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding. |
| Inspection | Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following:<br>• Examination / Inspection of source documentation and authorizations to verify transactions processed.<br>• Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures.<br>• Examination / Inspection of systems documentation, configurations, and settings; and<br>• Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions. |
| Observation | Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures. |

## Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." In the test result column of the Testing Matrices. Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the design and implementation of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

| Framework Code | Control Description | Test Applied by the Auditor | Test Results |
|---|---|---|---|
| 164.306(a) | Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors. | Inspected the Acceptable Use Policy and Data Protection Policy to determine that Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.<br><br>Inspected acknowledgement records to determine that these policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.306(a) | Phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures. | Inspected the Data Protection Policy and Information Disposal Procedure to determine that phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.<br><br>Inquired of the company to determine that no hardware decommissioning events were needed in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.306(a) | Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | Inspected the Acceptable Use Policy to determine that Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | No exceptions noted. |
| 164.306(a) | Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | Inspected the Data Classification Policy to determine that Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | No exceptions noted. |
| 164.306(a) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.306(a) | Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | Inspected the VPN enabled status, SSL status, and Encryption Policy to determine that remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | No exceptions noted. |
| 164.306(a) | Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password | Inspected the Password Policy and password configurations in place to determine that Phala Network has a documented policy outlining the minimum requirements for passwords used for | No exceptions noted. |

| | | | |
|---|---|---|---|
| | requirements are enforced for all systems in accordance with company policy. | authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | |
| 164.306(a) | Phala Network maintains a publicly available privacy policy/notice. | Inspected the public privacy policy to determine that Phala Network maintains a publicly available privacy policy/notice. | No exceptions noted. |
| 164.306(a) | Phala Network communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Phala Network provides notification to relevant parties of any changes to service commitments and system requirements. | Inspected the Terms and Conditions of Use including update records, and a services agreement to determine that Phala Network communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Phala Network provides notification to relevant parties of any changes to service commitments and system requirements. | No exceptions noted. |
| 164.306(a) | Phala Network has an established policy and procedures that governs the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has an established policy and procedures that governs the use of cryptographic controls. | No exceptions noted. |
| 164.306(a) | Anti-malware software is installed on all company-managed devices. | Inspected the anti-malware enabled status on workstations to determine that anti-malware software is installed on all company-managed devices. | No exceptions noted. |
| 164.306(a) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.306(a) | Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | Inspected the Code of Conduct to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter.<br><br>Inspected acknowledgement records to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | No exceptions noted. |
| 164.306(a) | Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | Inspected the Information Security Management System Plan to determine that management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.306(a) | Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | Inspected the Acceptable Use Policy to determine that Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | No exceptions noted. |
| 164.306(a) | Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | Inspected the Information Security Policy and training completion records to determine that Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | No exceptions noted. |
| 164.306(a) | Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | Inspected the Information Security Policy and company security policies to determine that Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | No exceptions noted. |
| 164.306(a) | Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected the Information Security Policy and Incident Response Plan to determine that Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | No exceptions noted. |
| 164.306(a) | Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | Inspected the Software Development Life Cycle Policy to determine that Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | No exceptions noted. |
| 164.306(a) | Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures. | Inspected the Incident Response Plan to determine that Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.<br><br>Inquired of company management to determine that no security incidents occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.306(a) | Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | Inspected the Business Continuity Plan to determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | scenario. | |
| 164.306(a) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.306(a) | Phala Network communicates its Privacy Policy on its public-facing website. | Inspected the public privacy policy to determine that Phala Network communicates its Privacy Policy on its public-facing website. | No exceptions noted. |
| 164.306(a) | Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | Inspected the Data Retention Policy to determine that Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | No exceptions noted. |
| 164.306(a) | Phala Network maintains policies and procedures that define allowable use and disclosure scenarios. | Inspected the Data Protection Policy to determine that Phala Network maintains policies and procedures that define allowable use and disclosure scenarios. | No exceptions noted. |
| 164.306(a) | Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | Inspected the Vulnerability Management Policy to determine that Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | No exceptions noted. |
| 164.306(a) | Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | Inspected the Asset Management Policy to determine that Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | No exceptions noted. |
| 164.306(a) | Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | No exceptions noted. |
| 164.306(a) | Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | Inspected the System Access Control Policy to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.<br><br>Inspected access configurations and records from a recent access review to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.306(a) | Phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | Inspected the Backup Policy to determine that phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | No exceptions noted. |
| 164.306(a) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.306(a) | Phala Network has an incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | Inspected the Incident Response Plan to determine that Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | No exceptions noted. |
| 164.306(a) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.306(a) | Phala Network communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Phala Network obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.). | Inspected the Data Processing Agreement to determine that Phala Network communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Phala Network obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.).. | No exceptions noted. |
| 164.306(a) | Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | No exceptions noted. |
| 164.306(a) | Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | disclosed. | |
| 164.306(a) | Phala Network has documented policies and procedures for erasure or destruction of information that has been identified for disposal. | Inspected the Information Disposal Procedure to determine that Phala Network has documented policies and procedures for erasure or destruction of information that has been identified for disposal. | No exceptions noted. |
| 164.306(b) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.306(b) | Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | Inspected the Acceptable Use Policy to determine that Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | No exceptions noted. |
| 164.306(b) | Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | Inspected the Information Security Policy and training completion records to determine that Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | No exceptions noted. |
| 164.306(b) | Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected the Information Security Policy and Incident Response Plan to determine that Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | No exceptions noted. |
| 164.306(b) | Phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | Inspected the Backup Policy to determine that phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | No exceptions noted. |
| 164.306(b) | Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | No exceptions noted. |
| 164.306(b) | Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | Inspected the Software Development Life Cycle Policy to determine that Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | No exceptions noted. |
| 164.306(b) | Phala Network has established and | Inspected the Asset Management Policy to | No exceptions noted. |

| | | | |
|---|---|---|---|
| | documented a policy that outlines requirements for the management and tracking of company assets. | determine that Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | |
| 164.306(b) | Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures. | Inspected the Incident Response Plan to determine that Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.<br><br>Inquired of company management to determine that no security incidents occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.306(b) | Phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures. | Inspected the Data Protection Policy and Information Disposal Procedure to determine that phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.<br><br>Inquired of the company to determine that no hardware decommissioning events were needed in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.306(b) | Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | Inspected the Business Continuity Plan to determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | No exceptions noted. |
| 164.306(b) | Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | Inspected the Vulnerability Management Policy to determine that Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | No exceptions noted. |
| 164.306(b) | Phala Network maintains policies and procedures that define allowable use and disclosure scenarios. | Inspected the Data Protection Policy to determine that Phala Network maintains policies and procedures that define allowable use and disclosure scenarios. | No exceptions noted. |
| 164.306(b) | Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | Inspected the Information Security Management System Plan to determine that management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | No exceptions noted. |
| 164.306(b) | Phala Network has documented policies and procedures for erasure or destruction of | Inspected the Information Disposal Procedure to determine that Phala Network has documented | No exceptions noted. |

| | | | |
|---|---|---|---|
| | information that has been identified for disposal. | policies and procedures for erasure or destruction of information that has been identified for disposal. | |
| 164.306(b) | Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | Inspected the Code of Conduct to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter.<br><br>Inspected acknowledgement records to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | No exceptions noted. |
| 164.306(b) | Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | Inspected the Data Retention Policy to determine that Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | No exceptions noted. |
| 164.306(b) | Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | Inspected the VPN enabled status, SSL status, and Encryption Policy to determine that remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | No exceptions noted. |
| 164.306(b) | Phala Network communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Phala Network obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.). | Inspected the Data Processing Agreement to determine that Phala Network communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Phala Network obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.).. | No exceptions noted. |
| 164.306(b) | Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | Inspected the Password Policy and password configurations in place to determine that Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | No exceptions noted. |
| 164.306(b) | Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.306(b) | Phala Network maintains a publicly available privacy policy/notice. | Inspected the public privacy policy to determine that Phala Network maintains a publicly available privacy policy/notice. | No exceptions noted. |
| 164.306(b) | Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | No exceptions noted. |
| 164.306(b) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.306(b) | Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | Inspected the Data Classification Policy to determine that Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | No exceptions noted. |
| 164.306(b) | Phala Network has an established policy and procedures that governs the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has an established policy and procedures that governs the use of cryptographic controls. | No exceptions noted. |
| 164.306(b) | Phala Network communicates its Privacy Policy on its public-facing website. | Inspected the public privacy policy to determine that Phala Network communicates its Privacy Policy on its public-facing website. | No exceptions noted. |
| 164.306(b) | Anti-malware software is installed on all company-managed devices. | Inspected the anti-malware enabled status on workstations to determine that anti-malware software is installed on all company-managed devices. | No exceptions noted. |
| 164.306(b) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.306(b) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.306(b) | Phala Network communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Phala Network provides notification to relevant parties of any changes to service commitments and system requirements. | Inspected the Terms and Conditions of Use including update records, and a services agreement to determine that Phala Network communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Phala Network provides notification to relevant parties of any changes to service commitments and system requirements. | No exceptions noted. |
| 164.306(b) | Phala Network has an incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | Inspected the Incident Response Plan to determine that Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | No exceptions noted. |
| 164.306(b) | Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | Inspected the Acceptable Use Policy to determine that Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | No exceptions noted. |
| 164.306(b) | Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors. | Inspected the Acceptable Use Policy and Data Protection Policy to determine that Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.<br><br>Inspected acknowledgement records to determine that these policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.306(b) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.306(b) | Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | Inspected the System Access Control Policy to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.<br><br>Inspected access configurations and records from a recent access review to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.306(b) | Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | Inspected the Information Security Policy and company security policies to determine that Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | No exceptions noted. |
| 164.306(c) | Anti-malware software is installed on all company-managed devices. | Inspected the anti-malware enabled status on workstations to determine that anti-malware software is installed on all company-managed devices. | No exceptions noted. |
| 164.306(c) | Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | Inspected the Vulnerability Management Policy to determine that Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | No exceptions noted. |
| 164.306(c) | Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors. | Inspected the Acceptable Use Policy and Data Protection Policy to determine that Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.<br><br>Inspected acknowledgement records to determine that these policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.306(c) | Phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | Inspected the Backup Policy to determine that phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | No exceptions noted. |
| 164.306(c) | Phala Network communicates its Privacy Policy on its public-facing website. | Inspected the public privacy policy to determine that Phala Network communicates its Privacy Policy on its public-facing website. | No exceptions noted. |
| 164.306(c) | Phala Network communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Phala Network obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.). | Inspected the Data Processing Agreement to determine that Phala Network communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Phala Network obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.).. | No exceptions noted. |
| 164.306(c) | Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed | Inspected the Incident Response Plan to determine that Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response | No exceptions noted. |

| | | | |
|---|---|---|---|
| | periodically and updated as needed according to lessons learned from previous incidents and industry developments. | plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | |
| 164.306(c) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.306(c) | Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | Inspected the Data Retention Policy to determine that Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | No exceptions noted. |
| 164.306(c) | Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | Inspected the Asset Management Policy to determine that Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | No exceptions noted. |
| 164.306(c) | Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected the Information Security Policy and Incident Response Plan to determine that Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | No exceptions noted. |
| 164.306(c) | Phala Network has an established policy and procedures that governs the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has an established policy and procedures that governs the use of cryptographic controls. | No exceptions noted. |
| 164.306(c) | Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | Inspected the Information Security Management System Plan to determine that management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | No exceptions noted. |
| 164.306(c) | Phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures. | Inspected the Data Protection Policy and Information Disposal Procedure to determine that phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.<br><br>Inquired of the company to determine that no hardware decommissioning events were needed in the last year. | Not tested. Control activity did not occur during the audit. |

| | | | |
|---|---|---|---|
| 164.306(c) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.306(c) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.306(c) | Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | No exceptions noted. |
| 164.306(c) | Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | Inspected the Software Development Life Cycle Policy to determine that Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | No exceptions noted. |
| 164.306(c) | Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures. | Inspected the Incident Response Plan to determine that Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.<br><br>Inquired of company management to determine that no security incidents occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.306(c) | Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | Inspected the Information Security Policy and company security policies to determine that Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | No exceptions noted. |
| 164.306(c) | Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | Inspected the Code of Conduct to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter.<br><br>Inspected acknowledgement records to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | No exceptions noted. |
| 164.306(c) | Phala Network has a documented disaster | Inspected the Business Continuity Plan to | No exceptions noted. |

| | | | |
|---|---|---|---|
| | recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | |
| 164.306(c) | Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | Inspected the VPN enabled status, SSL status, and Encryption Policy to determine that remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | No exceptions noted. |
| 164.306(c) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.306(c) | Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | Inspected the Acceptable Use Policy to determine that Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | No exceptions noted. |
| 164.306(c) | Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | Inspected the Acceptable Use Policy to determine that Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | No exceptions noted. |
| 164.306(c) | Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | Inspected the Data Classification Policy to determine that Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | No exceptions noted. |
| 164.306(c) | Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | Inspected the Password Policy and password configurations in place to determine that Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | No exceptions noted. |
| 164.306(c) | Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | No exceptions noted. |
| 164.306(c) | Phala Network maintains a publicly available | Inspected the public privacy policy to determine | No exceptions noted. |

| | | | |
|---|---|---|---|
| | privacy policy/notice. | that Phala Network maintains a publicly available privacy policy/notice. | |
| 164.306(c) | Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | Inspected the System Access Control Policy to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.<br><br>Inspected access configurations and records from a recent access review to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | No exceptions noted. |
| 164.306(c) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.306(c) | Phala Network has documented policies and procedures for erasure or destruction of information that has been identified for disposal. | Inspected the Information Disposal Procedure to determine that Phala Network has documented policies and procedures for erasure or destruction of information that has been identified for disposal. | No exceptions noted. |
| 164.306(c) | Phala Network communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Phala Network provides notification to relevant parties of any changes to service commitments and system requirements. | Inspected the Terms and Conditions of Use including update records, and a services agreement to determine that Phala Network communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Phala Network provides notification to relevant parties of any changes to service commitments and system requirements. | No exceptions noted. |
| 164.306(c) | Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | No exceptions noted. |
| 164.306(c) | Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher | Inspected the Information Security Policy and training completion records to determine that Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete | No exceptions noted. |

| | | | |
|---|---|---|---|
| | training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | |
| 164.306(c) | Phala Network maintains policies and procedures that define allowable use and disclosure scenarios. | Inspected the Data Protection Policy to determine that Phala Network maintains policies and procedures that define allowable use and disclosure scenarios. | No exceptions noted. |
| 164.306(d) | Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | Inspected the Information Security Management System Plan to determine that management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | No exceptions noted. |
| 164.306(d) | Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | No exceptions noted. |
| 164.306(d) | Anti-malware software is installed on all company-managed devices. | Inspected the anti-malware enabled status on workstations to determine that anti-malware software is installed on all company-managed devices. | No exceptions noted. |
| 164.306(d) | Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | Inspected the Data Retention Policy to determine that Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | No exceptions noted. |
| 164.306(d) | Phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures. | Inspected the Data Protection Policy and Information Disposal Procedure to determine that phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.<br><br>Inquired of the company to determine that no hardware decommissioning events were needed in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.306(d) | Phala Network maintains a publicly available privacy policy/notice. | Inspected the public privacy policy to determine that Phala Network maintains a publicly available privacy policy/notice. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.306(d) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.306(d) | Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | Inspected the Data Classification Policy to determine that Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | No exceptions noted. |
| 164.306(d) | Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | No exceptions noted. |
| 164.306(d) | Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | Inspected the Software Development Life Cycle Policy to determine that Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | No exceptions noted. |
| 164.306(d) | Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | Inspected the Code of Conduct to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter.<br><br>Inspected acknowledgement records to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | No exceptions noted. |
| 164.306(d) | Phala Network maintains policies and procedures that define allowable use and disclosure scenarios. | Inspected the Data Protection Policy to determine that Phala Network maintains policies and procedures that define allowable use and disclosure scenarios. | No exceptions noted. |
| 164.306(d) | Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | Inspected the Vulnerability Management Policy to determine that Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | No exceptions noted. |
| 164.306(d) | Phala Network evaluates security events to | Inspected the Incident Response Plan to determine | Not tested. Control |

| | | | |
|---|---|---|---|
| | determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures. | that Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.<br><br>Inquired of company management to determine that no security incidents occurred in the last year. | activity did not occur during the audit. |
| 164.306(d) | Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | Inspected the Password Policy and password configurations in place to determine that Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | No exceptions noted. |
| 164.306(d) | Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | Inspected the VPN enabled status, SSL status, and Encryption Policy to determine that remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | No exceptions noted. |
| 164.306(d) | Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | Inspected the Information Security Policy and company security policies to determine that Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | No exceptions noted. |
| 164.306(d) | Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | Inspected the System Access Control Policy to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.<br><br>Inspected access configurations and records from a recent access review to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | No exceptions noted. |
| 164.306(d) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.306(d) | Phala Network has developed and documented a policy that outlines requirements for access | Inspected the System Access Control Policy to determine that Phala Network has developed and | No exceptions noted. |

| | | | |
|---|---|---|---|
| | control. | documented a policy that outlines requirements for access control. | |
| 164.306(d) | Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | No exceptions noted. |
| 164.306(d) | Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | Inspected the Asset Management Policy to determine that Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | No exceptions noted. |
| 164.306(d) | Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | Inspected the Business Continuity Plan to determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | No exceptions noted. |
| 164.306(d) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.306(d) | Phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | Inspected the Backup Policy to determine that phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | No exceptions noted. |
| 164.306(d) | Phala Network communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Phala Network obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.). | Inspected the Data Processing Agreement to determine that Phala Network communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Phala Network obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.).. | No exceptions noted. |
| 164.306(d) | Phala Network communicates its Privacy Policy on its public-facing website. | Inspected the public privacy policy to determine that Phala Network communicates its Privacy Policy on its public-facing website. | No exceptions noted. |
| 164.306(d) | Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | Inspected the Incident Response Plan to determine that Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | No exceptions noted. |
| 164.306(d) | Phala Network has an established policy and | Inspected the Encryption Policy to determine that | No exceptions noted. |

| | | | |
|---|---|---|---|
| | procedures that governs the use of cryptographic controls. | Phala Network has an established policy and procedures that governs the use of cryptographic controls. | |
| 164.306(d) | Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected the Information Security Policy and Incident Response Plan to determine that Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | No exceptions noted. |
| 164.306(d) | Phala Network communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Phala Network provides notification to relevant parties of any changes to service commitments and system requirements. | Inspected the Terms and Conditions of Use including update records, and a services agreement to determine that Phala Network communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Phala Network provides notification to relevant parties of any changes to service commitments and system requirements. | No exceptions noted. |
| 164.306(d) | Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | Inspected the Acceptable Use Policy to determine that Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | No exceptions noted. |
| 164.306(d) | Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | Inspected the Acceptable Use Policy to determine that Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | No exceptions noted. |
| 164.306(d) | Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | Inspected the Information Security Policy and training completion records to determine that Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | No exceptions noted. |
| 164.306(d) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.306(d) | Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These | Inspected the Acceptable Use Policy and Data Protection Policy to determine that Phala Network Management has approved all policies that detail | No exceptions noted. |

| | | | |
|---|---|---|---|
| | policies are accessible to all employees and contractors. | how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.<br><br>Inspected acknowledgement records to determine that these policies are accessible to all employees and contractors. | |
| 164.306(d) | Phala Network has documented policies and procedures for erasure or destruction of information that has been identified for disposal. | Inspected the Information Disposal Procedure to determine that Phala Network has documented policies and procedures for erasure or destruction of information that has been identified for disposal. | No exceptions noted. |
| 164.306(e) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.306(e) | Phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | Inspected the Backup Policy to determine that phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | No exceptions noted. |
| 164.306(e) | Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | Inspected the Software Development Life Cycle Policy to determine that Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | No exceptions noted. |
| 164.306(e) | Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | Inspected the Acceptable Use Policy to determine that Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | No exceptions noted. |
| 164.306(e) | Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | Inspected the Information Security Management System Plan to determine that management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | No exceptions noted. |
| 164.306(e) | Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | Inspected the Data Classification Policy to determine that Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | No exceptions noted. |
| 164.306(e) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | access control. | |
| 164.306(e) | Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.). | Inspected the Information Security Policy to determine that management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.).<br><br>Inspected review and approval monitoring records to determine that management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.). | No exceptions noted. |
| 164.306(e) | Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | Inspected the Acceptable Use Policy to determine that Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | No exceptions noted. |
| 164.306(e) | Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected the Information Security Policy and Incident Response Plan to determine that Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | No exceptions noted. |
| 164.306(e) | Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | Inspected the Information Security Policy and training completion records to determine that Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | No exceptions noted. |
| 164.306(e) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.306(e) | Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, | Inspected the System Access Control Policy to determine that Phala Network authorizes access to information resources, including data and the | No exceptions noted. |

| | | | |
|---|---|---|---|
| | based on the principle of least privilege. | systems that store or process sensitive data, based on the principle of least privilege.<br><br>Inspected access configurations and records from a recent access review to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | |
| 164.306(e) | Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | Inspected the Incident Response Plan to determine that Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | No exceptions noted. |
| 164.306(e) | Phala Network's management reviews the privacy notice to ensure that the privacy notice is accurate. | Inspected the Phala Cloud Annual Privacy Policy Review Report to determine that Phala Network's management reviews the privacy notice to ensure that the privacy notice is accurate.<br><br>Inspected the Privacy Policy which includes a last updated date to determine that Phala Network's management reviews the privacy notice to ensure that the privacy notice is accurate. | No exceptions noted. |
| 164.306(e) | Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | Inspected the VPN enabled status, SSL status, and Encryption Policy to determine that remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | No exceptions noted. |
| 164.306(e) | Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | Inspected the Vulnerability Management Policy to determine that Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | No exceptions noted. |
| 164.306(e) | Phala Network communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Phala Network obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.). | Inspected the Data Processing Agreement to determine that Phala Network communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Phala Network obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.).. | No exceptions noted. |
| 164.306(e) | Phala Network communicates its Privacy Policy on its public-facing website. | Inspected the public privacy policy to determine that Phala Network communicates its Privacy | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | Policy on its public-facing website. | |
| 164.306(e) | Phala Network maintains policies and procedures that define allowable use and disclosure scenarios. | Inspected the Data Protection Policy to determine that Phala Network maintains policies and procedures that define allowable use and disclosure scenarios. | No exceptions noted. |
| 164.306(e) | Phala Network's management reviews the online privacy policy and/or notice at least annually to validate its continued suitability and accuracy. The online privacy policy/notice includes the date it was last updated. Phala Network notifies customers of changes to the privacy notice and the nature of the changes, including when personal information will be used for new purposes not previously identified. | Inspected the Phala Cloud Annual Privacy Policy Review Report and Privacy Policy to determine that Phala Network's management reviews the online privacy policy and/or notice at least annually to validate its continued suitability and accuracy. The online privacy policy/notice includes the date it was last updated. Phala Network notifies customers of changes to the privacy notice and the nature of the changes, including when personal information will be used for new purposes not previously identified. | No exceptions noted. |
| 164.306(e) | Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | No exceptions noted. |
| 164.306(e) | Executive management meets on a quarterly basis to review compliance with privacy practices and privacy regulations. | Inspected the company's Information Security Management System Plan and formalized review documentation to determine that executive management meets on a quarterly basis to review compliance with privacy practices and privacy regulations.<br><br>Inquired of the company to determine that quarterly privacy practices and privacy regulation reviews were conducted but not formally documented and evidence of quarterly reviews isn't available. | Exceptions noted. |
| 164.306(e) | Phala Network has documented policies and procedures for erasure or destruction of information that has been identified for disposal. | Inspected the Information Disposal Procedure to determine that Phala Network has documented policies and procedures for erasure or destruction of information that has been identified for disposal. | No exceptions noted. |
| 164.306(e) | Phala Network communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Phala Network provides notification to relevant parties of any changes to service commitments and system requirements. | Inspected the Terms and Conditions of Use including update records, and a services agreement to determine that Phala Network communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Phala Network provides notification to relevant parties of any changes to service commitments and system requirements. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.306(e) | Phala Network maintains a publicly available privacy policy/notice. | Inspected the public privacy policy to determine that Phala Network maintains a publicly available privacy policy/notice. | No exceptions noted. |
| 164.306(e) | Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | No exceptions noted. |
| 164.306(e) | Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | Inspected the Password Policy and password configurations in place to determine that Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | No exceptions noted. |
| 164.306(e) | Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | No exceptions noted. |
| 164.306(e) | Phala Network has an established policy and procedures that governs the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has an established policy and procedures that governs the use of cryptographic controls. | No exceptions noted. |
| 164.306(e) | Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | Inspected the Asset Management Policy to determine that Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | No exceptions noted. |
| 164.306(e) | A documented network diagram is in place to document system boundaries and connections to external networks. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment. | Inspected the network diagram including review date to determine that a documented network diagram is in place to document system boundaries and connections to external networks. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment. | No exceptions noted. |
| 164.306(e) | Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures. | Inspected the Incident Response Plan to determine that Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.<br><br>Inquired of company management to determine that no security incidents occurred in the last year. | Not tested. Control activity did not occur during the audit. |

| | | | |
|---|---|---|---|
| 164.306(e) | Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | Inspected the Information Security Policy and company security policies to determine that Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | No exceptions noted. |
| 164.306(e) | Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | Inspected the Code of Conduct to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter.<br><br>Inspected acknowledgement records to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | No exceptions noted. |
| 164.306(e) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.306(e) | Anti-malware software is installed on all company-managed devices. | Inspected the anti-malware enabled status on workstations to determine that anti-malware software is installed on all company-managed devices. | No exceptions noted. |
| 164.306(e) | Phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures. | Inspected the Data Protection Policy and Information Disposal Procedure to determine that phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.<br><br>Inquired of the company to determine that no hardware decommissioning events were needed in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.306(e) | Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | Inspected the Business Continuity Plan to determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | No exceptions noted. |
| 164.306(e) | Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes | Inspected the System Access Control Policy and most recent Access Review records to determine that management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated | No exceptions noted. |

| | | | |
|---|---|---|---|
| | validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | |
| 164.306(e) | Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors. | Inspected the Acceptable Use Policy and Data Protection Policy to determine that Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.<br><br>Inspected acknowledgement records to determine that these policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.306(e) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.306(e) | Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | Inspected the Data Retention Policy to determine that Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.308(a)(1)(i) | Anti-malware software is installed on all company-managed devices. | Inspected the anti-malware enabled status on workstations to determine that anti-malware software is installed on all company-managed devices. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | Inspected the Acceptable Use Policy to determine that Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.308(a)(1)(i) | Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | Inspected the Code of Conduct to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter.<br><br>Inspected acknowledgement records to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | No exceptions noted. |
| 164.308(a)(1)(i) | Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | Inspected the Information Security Management System Plan to determine that management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | Inspected the Incident Response Plan to determine that Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has an established policy and procedures that governs the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has an established policy and procedures that governs the use of cryptographic controls. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | Inspected the Password Policy and password configurations in place to determine that Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | Inspected the System Access Control Policy to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | Inspected access configurations and records from a recent access review to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | |
| 164.308(a)(1)(i) | Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | Inspected the Information Security Policy and company security policies to determine that Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | Inspected the Data Retention Policy to determine that Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures. | Inspected the Data Protection Policy and Information Disposal Procedure to determine that phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.<br><br>Inquired of the company to determine that no hardware decommissioning events were needed in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.308(a)(1)(i) | Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | Inspected the Asset Management Policy to determine that Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | Inspected the Vulnerability Management Policy to determine that Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has documented policies and procedures for erasure or destruction of information that has been identified for disposal. | Inspected the Information Disposal Procedure to determine that Phala Network has documented policies and procedures for erasure or destruction of information that has been identified for disposal. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, | Inspected the Incident Response Plan to determine that Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, | Not tested. Control activity did not occur during the audit. |

| | | | |
|---|---|---|---|
| | eradicated, communicated, and resolved in accordance with company policies and procedures. | tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.<br><br>Inquired of company management to determine that no security incidents occurred in the last year. | |
| 164.308(a)(1)(i) | Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | Inspected the Software Development Life Cycle Policy to determine that Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors. | Inspected the Acceptable Use Policy and Data Protection Policy to determine that Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.<br><br>Inspected acknowledgement records to determine that these policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | Inspected the Acceptable Use Policy to determine that Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | Inspected the Business Continuity Plan to determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has established a data | Inspected the Data Classification Policy to | No exceptions noted. |

| | | | |
|---|---|---|---|
| | classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | determine that Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | |
| 164.308(a)(1)(i) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | Inspected the Information Security Policy and training completion records to determine that Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | No exceptions noted. |
| 164.308(a)(1)(i) | Phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | Inspected the Backup Policy to determine that phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | No exceptions noted. |
| 164.308(a)(1)(ii)(A) | Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | No exceptions noted. |
| 164.308(a)(1)(ii)(A) | Phala Network conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies. | Inspected the vulnerability scan dashboard, a report, and Vulnerability Management Policy to determine that Phala Network conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies. | No exceptions noted. |
| 164.308(a)(1)(ii)(A) | An external penetration test of production environments is performed by an independent third party periodically or after any significant infrastructure or application changes. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies. | Inspected the Vulnerability Management Policy and latest penetration test report to determine that an external penetration test of production environments is performed by an independent third party periodically or after any significant infrastructure or application changes. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.308(a)(1)(ii)(A) | Phala Network's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. | No exceptions noted. |
| 164.308(a)(1)(ii)(A) | Phala Network conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented (e.g., in a risk register). | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network conducts risks assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented (e.g., in a risk register). | No exceptions noted. |
| 164.308(a)(1)(ii)(B) | Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | No exceptions noted. |
| 164.308(a)(1)(ii)(B) | Phala Network conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented (e.g., in a risk register). | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network conducts risks assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented (e.g., in a risk register). | No exceptions noted. |
| 164.308(a)(1)(ii)(B) | Phala Network's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities. | No exceptions noted. |
| 164.308(a)(1)(ii)(B) | An external penetration test of production environments is performed by an independent third party periodically or after any significant infrastructure or application changes. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies. | Inspected the Vulnerability Management Policy and latest penetration test report to determine that an external penetration test of production environments is performed by an independent third party periodically or after any significant infrastructure or application changes. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.308(a)(1)(ii)(B) | Phala Network conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies. | Inspected the vulnerability scan dashboard, a report, and Vulnerability Management Policy to determine that Phala Network conducts vulnerability scans of the production environment as dictated by company policy and compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies. | No exceptions noted. |
| 164.308(a)(1)(ii)(C) | Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | Inspected the Information Security Policy and company security policies to determine that Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | No exceptions noted. |
| 164.308(a)(1)(ii)(D) | Phala Network performs a review of information system activities on regular intervals | Inspected the Logging and Monitoring Policy, compliance monitoring system, access review, and monitoring dashboard to determine that Phala Network performs a review of information system activities on regular intervals. | No exceptions noted. |
| 164.308(a)(1)(ii)(D) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.308(a)(2) | Phala Network has identified and documented skill and competence requirements for personnel that contribute to the development, implementation and oversight of its management system(s) and retains documented evidence of competence. | Inspected the Information Security Management System Plan and screening process in place to determine that Phala Network has identified and documented skill and competence requirements for personnel that contribute to the development, implementation and oversight of its management system(s) and retains documented evidence of competence. | No exceptions noted. |
| 164.308(a)(2) | Phala Network has formally assigned responsibility for information security in the organization to a Chief Information Security Officer or other security-knowledgeable member of management. | Inspected the Information Security Policy to determine that Phala Network has formally assigned responsibility for information security in the organization to a Chief Information Security Officer or other security-knowledgeable member of management. | No exceptions noted. |
| 164.308(a)(2) | Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | Inspected the Information Security Policy and company security policies to determine that Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | No exceptions noted. |
| 164.308(a)(3)(i) | Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | Inspected the Access Control Policy to determine that Administrative or privileged access to systems, resources, and functions is restricted to authorized | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | personnel.<br><br>Inspected the access review and user configurations to determine that administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | |
| 164.308(a)(3)(ii)(A) | Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | Inspected the System Access Control Policy and most recent Access Review records to determine that management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | No exceptions noted. |
| 164.308(a)(3)(ii)(A) | Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | Inspected the Access Control Policy to determine that Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.<br><br>Inspected the access review and user configurations to determine that administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | No exceptions noted. |
| 164.308(a)(3)(ii)(A) | Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | Inspected the access provision register and System Access Control Policy to determine that access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | No exceptions noted. |
| 164.308(a)(3)(ii)(A) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.308(a)(3)(ii)(A) | Authentication to systems requires the use of unique identities. | Inspected a list of employees to determine that authentication to systems requires the use of unique identities. | No exceptions noted. |
| 164.308(a)(3)(ii)(A) | Phala Network uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | Inspected the System Access Control Policy and termination checklist to determine that Phala Network uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | No exceptions noted. |
| 164.308(a)(3)(ii)(B) | Background checks are conducted on eligible | Inspected a list of personnel with completed | No exceptions noted. |

| | | | |
|---|---|---|---|
| | personnel (employees and third parties as deemed necessary by the organization) prior to hire as permitted by local laws. | background checks to determine that background checks are conducted on eligible personnel (employees and third parties as deemed necessary by the organization) prior to hire as permitted by local laws. | |
| 164.308(a)(3)(ii)(B) | Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | Inspected the access provision register and System Access Control Policy to determine that access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | No exceptions noted. |
| 164.308(a)(3)(ii)(B) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.308(a)(3)(ii)(B) | Authentication to systems requires the use of unique identities. | Inspected a list of employees to determine that authentication to systems requires the use of unique identities. | No exceptions noted. |
| 164.308(a)(3)(ii)(C) | System and physical access is revoked within one business day of the effective termination date for terminated users (including employees, third parties and vendors, and other personnel). | Inspected the System Access Control Policy to determine that System and physical access is revoked within one business day of effective termination date for terminated users (including employees, third parties and vendors, and other personnel).<br><br>Inspected revocation records within SLA to determine that terminated users must have access revoked within one business day. | No exceptions noted. |
| 164.308(a)(3)(ii)(C) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.308(a)(3)(ii)(C) | Phala Network uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | Inspected the System Access Control Policy and termination checklist to determine that Phala Network uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | No exceptions noted. |
| 164.308(a)(4)(i) | Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as | Inspected the System Access Control Policy and most recent Access Review records to determine that management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes | No exceptions noted. |

| | | | |
|---|---|---|---|
| | necessary. Changes resulting from the review, if any, are documented and implemented. | validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | |
| 164.308(a)(4)(i) | Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | Inspected the access provision register and System Access Control Policy to determine that access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | No exceptions noted. |
| 164.308(a)(4)(i) | Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | Inspected the Access Control Policy to determine that Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.<br><br>Inspected the access review and user configurations to determine that administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | No exceptions noted. |
| 164.308(a)(4)(i) | Phala Network has an established key management process in place to support the organization's use of cryptographic techniques. | Inspected the Encryption Policy and company encryption in transit status to determine that Phala Network has an established key management process in place to support the organization's use of cryptographic techniques. | No exceptions noted. |
| 164.308(a)(4)(i) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.308(a)(4)(i) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.308(a)(4)(i) | System and physical access is revoked within one business day of the effective termination date for terminated users (including employees, third parties and vendors, and other personnel). | Inspected the System Access Control Policy to determine that System and physical access is revoked within one business day of effective termination date for terminated users (including employees, third parties and vendors, and other personnel).<br><br>Inspected revocation records within SLA to determine that terminated users must have access revoked within one business day. | No exceptions noted. |
| 164.308(a)(4)(i) | Phala Network authorizes access to information resources, including data and the | Inspected the System Access Control Policy to determine that Phala Network authorizes access to | No exceptions noted. |

| | | | |
|---|---|---|---|
| | systems that store or process sensitive data, based on the principle of least privilege. | information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.<br><br>Inspected access configurations and records from a recent access review to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | |
| 164.308(a)(4)(i) | Phala Network uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | Inspected the System Access Control Policy and termination checklist to determine that Phala Network uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | No exceptions noted. |
| 164.308(a)(4)(ii)(A) | Phala Network has an established key management process in place to support the organization's use of cryptographic techniques. | Inspected the Encryption Policy and company encryption in transit status to determine that Phala Network has an established key management process in place to support the organization's use of cryptographic techniques. | No exceptions noted. |
| 164.308(a)(4)(ii)(A) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.308(a)(4)(ii)(A) | Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | Inspected the access provision register and System Access Control Policy to determine that access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | No exceptions noted. |
| 164.308(a)(4)(ii)(A) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.308(a)(4)(ii)(A) | Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | Inspected the System Access Control Policy to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.<br><br>Inspected access configurations and records from a recent access review to determine that Phala | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | |
| 164.308(a)(4)(ii)(A) | System and physical access is revoked within one business day of the effective termination date for terminated users (including employees, third parties and vendors, and other personnel). | Inspected the System Access Control Policy to determine that System and physical access is revoked within one business day of effective termination date for terminated users (including employees, third parties and vendors, and other personnel).<br><br>Inspected revocation records within SLA to determine that terminated users must have access revoked within one business day. | No exceptions noted. |
| 164.308(a)(4)(ii)(A) | Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | Inspected the Access Control Policy to determine that Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.<br><br>Inspected the access review and user configurations to determine that administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | No exceptions noted. |
| 164.308(a)(4)(ii)(A) | A documented architectural diagram is in place to document system boundaries and support the functioning of internal control. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment. | Inspected the architectural diagram to determine that a documented architectural diagram is in place to document system boundaries and support the functioning of internal control. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment. | No exceptions noted. |
| 164.308(a)(4)(ii)(A) | Phala Network uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | Inspected the System Access Control Policy and termination checklist to determine that Phala Network uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | No exceptions noted. |
| 164.308(a)(4)(ii)(A) | Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | Inspected the System Access Control Policy and most recent Access Review records to determine that management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | No exceptions noted. |
| 164.308(a)(4)(ii)(A) | Phala Network has identified and documented | Inspected the Asset Management Policy and | No exceptions noted. |

| | | | |
|---|---|---|---|
| | baseline security configuration standards for all system components in accordance with industry-accepted hardening standards or vendor recommendations. These standards are reviewed periodically and updated as needed (e.g., when vulnerabilities are identified) and verified to be in place before or immediately after a production system component is installed or modified (e.g., through infrastructure as code, configuration checklists, etc.). | baseline configuration and hardening standards documentation to determine that Phala Network has identified and documented baseline security configuration standards for all system components in accordance with industry-accepted hardening standards or vendor recommendations. These standards are reviewed periodically and updated as needed (e.g., when vulnerabilities are identified) and verified to be in place before or immediately after a production system component is installed or modified (e.g., through infrastructure as code, configuration checklists, etc.). | |
| 164.308(a)(4)(ii)(B) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.308(a)(4)(ii)(B) | Phala Network uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | Inspected the System Access Control Policy and termination checklist to determine that Phala Network uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | No exceptions noted. |
| 164.308(a)(4)(ii)(B) | Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | Inspected the Access Control Policy to determine that Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.<br><br>Inspected the access review and user configurations to determine that administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | No exceptions noted. |
| 164.308(a)(4)(ii)(B) | System and physical access is revoked within one business day of the effective termination date for terminated users (including employees, third parties and vendors, and other personnel). | Inspected the System Access Control Policy to determine that System and physical access is revoked within one business day of effective termination date for terminated users (including employees, third parties and vendors, and other personnel).<br><br>Inspected revocation records within SLA to determine that terminated users must have access revoked within one business day. | No exceptions noted. |
| 164.308(a)(4)(ii)(B) | Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | Inspected the access provision register and System Access Control Policy to determine that access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.308(a)(4)(ii)(B) | Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | Inspected the System Access Control Policy to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.<br><br>Inspected access configurations and records from a recent access review to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | No exceptions noted. |
| 164.308(a)(4)(ii)(B) | Phala Network has an established key management process in place to support the organization's use of cryptographic techniques. | Inspected the Encryption Policy and company encryption in transit status to determine that Phala Network has an established key management process in place to support the organization's use of cryptographic techniques. | No exceptions noted. |
| 164.308(a)(4)(ii)(B) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.308(a)(4)(ii)(B) | Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | Inspected the System Access Control Policy and most recent Access Review records to determine that management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | No exceptions noted. |
| 164.308(a)(4)(ii)(C) | Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | Inspected the Access Control Policy to determine that Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.<br><br>Inspected the access review and user configurations to determine that administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | No exceptions noted. |
| 164.308(a)(4)(ii)(C) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.308(a)(4)(ii)(C) | Phala Network uses a termination checklist to | Inspected the System Access Control Policy and | No exceptions noted. |

| | | | |
|---|---|---|---|
| | ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | termination checklist to determine that Phala Network uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | |
| 164.308(a)(4)(ii)(C) | System and physical access is revoked within one business day of the effective termination date for terminated users (including employees, third parties and vendors, and other personnel). | Inspected the System Access Control Policy to determine that System and physical access is revoked within one business day of effective termination date for terminated users (including employees, third parties and vendors, and other personnel).<br><br>Inspected revocation records within SLA to determine that terminated users must have access revoked within one business day. | No exceptions noted. |
| 164.308(a)(4)(ii)(C) | Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | Inspected the System Access Control Policy to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.<br><br>Inspected access configurations and records from a recent access review to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | No exceptions noted. |
| 164.308(a)(4)(ii)(C) | Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | Inspected the System Access Control Policy and most recent Access Review records to determine that management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | No exceptions noted. |
| 164.308(a)(4)(ii)(C) | Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | Inspected the access provision register and System Access Control Policy to determine that access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | No exceptions noted. |
| 164.308(a)(5)(i) | Phala Network has established a training program for the use and disclosure of protected health information (PHI) to help personnel understand their obligations and | Inspected the PHI training completion status to determine that Phala Network has established a training program for the use and disclosure of protected health information (PHI) to help | No exceptions noted. |

| | | | |
|---|---|---|---|
| | responsibilities related to HIPAA. All eligible members of the workforce are required to complete this training during onboarding and annually thereafter. | personnel understand their obligations and responsibilities related to HIPAA. All eligible members of the workforce are required to complete this training during onboarding and annually thereafter. | |
| 164.308(a)(5)(i) | Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | Inspected the Information Security Policy and company security policies to determine that Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | No exceptions noted. |
| 164.308(a)(5)(i) | Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | Inspected the Information Security Policy and training completion records to determine that Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | No exceptions noted. |
| 164.308(a)(5)(ii)(A) | Phala Network has documented procedures for periodic communication of security updates and reminders to all personnel, and other interested parties when appropriate | Inspected the security communication and personnel training completion status to determine that Phala Network has documented procedures for periodic communication of security updates and reminders to all personnel, and other interested parties when appropriate | No exceptions noted. |
| 164.308(a)(5)(ii)(B) | Anti-malware software is installed on all company-managed devices. | Inspected the anti-malware enabled status on workstations to determine that anti-malware software is installed on all company-managed devices. | No exceptions noted. |
| 164.308(a)(5)(ii)(B) | Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | Inspected the Acceptable Use Policy to determine that Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | No exceptions noted. |
| 164.308(a)(5)(ii)(B) | An intrusion detection system (IDS)/intrusion prevention system (IPS) or equivalent is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected. | Inspected the Logging and Monitoring Policy and AWS GuardDuty in place to determine that an intrusion detection system (IDS)/intrusion prevention system (IPS) or equivalent is in place to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity and is configured to alert personnel when a potential intrusion is detected. | No exceptions noted. |
| 164.308(a)(5)(ii)(C) | Phala Network uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner. | Inspected the Datadog monitoring dashboard to determine that Phala Network uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | timely manner. | |
| 164.308(a)(5)(ii)(C) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.308(a)(5)(ii)(C) | Phala Network has a defined plan for event logging that establishes the required criteria for logs, protection of logged information, and clock synchronization. | Inspected the Logging and Monitoring Policy, access review records, and clock synchronization configurations to determine that Phala Network has a defined plan for event logging that establishes the required criteria for logs, protection of logged information, and clock synchronization. | No exceptions noted. |
| 164.308(a)(5)(ii)(D) | Phala Network has implemented technical measures to protect stored user passwords for the system (e.g., encryption, hashing, salting, etc.). | Inspected the Data Protection Policy and hashing in place to determine that Phala Network has implemented technical measures to protect stored user passwords for the system (e.g., encryption, hashing, salting, etc.). | No exceptions noted. |
| 164.308(a)(5)(ii)(D) | A password manager is installed on all company-managed devices. | Inspected the Password Policy and a list of workstations with password manager enabled to determine that a password manager is installed on all company-managed devices. | No exceptions noted. |
| 164.308(a)(5)(ii)(D) | Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | Inspected the Password Policy and password configurations in place to determine that Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | No exceptions noted. |
| 164.308(a)(6)(i) | Phala Network has identified and documented roles and responsibilities for incident management (e.g., roles and responsibilities for invoking the incident management process, incident leads, incident handlers, communication coordinators, technical advisors, legal advisors, etc.). | Inspected the Incident Response Plan and documentation to determine that Phala Network has identified and documented roles and responsibilities for incident management (e.g., roles and responsibilities for invoking the incident management process, incident leads, incident handlers, communication coordinators, technical advisors, legal advisors, etc.). | No exceptions noted. |
| 164.308(a)(6)(i) | Phala Network performs a test of all components of the incident response plan and procedures at least annually through different mechanisms (e.g., walk-through or tabletop exercises, simulations, etc.). The documented plan and procedures are updated if necessary based on the results of the test. | Inspected the Incident Response Plan and latest Incident Response Test to determine that Phala Network performs a test of all components of the incident response plan and procedures at least annually through different mechanisms (e.g., walk-through or tabletop exercises, simulations, etc.). The documented plan and procedures are updated if necessary based on the results of the test. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.308(a)(6)(i) | Phala Network has incident management procedures that include detailed instructions on how to escalate a suspected incident to the Information Security Team and, when necessary, to the Privacy or Legal department. Phala Network has a standard incident report template that must be completed for each incident. | Inspected the Incident Response Plan to determine that Phala Network has incident management procedures that include detailed instructions on how to escalate a suspected incident to the Information Security Team and, when necessary, to the Privacy or Legal department. Phala Network has a standard incident report template that must be completed for each incident.<br><br>Inquired of company management to determine that no incidents occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.308(a)(6)(i) | Phala Network has an incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | Inspected the Incident Response Plan to determine that Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | No exceptions noted. |
| 164.308(a)(6)(ii) | Phala Network has identified and documented roles and responsibilities for incident management (e.g., roles and responsibilities for invoking the incident management process, incident leads, incident handlers, communication coordinators, technical advisors, legal advisors, etc.). | Inspected the Incident Response Plan and documentation to determine that Phala Network has identified and documented roles and responsibilities for incident management (e.g., roles and responsibilities for invoking the incident management process, incident leads, incident handlers, communication coordinators, technical advisors, legal advisors, etc.). | No exceptions noted. |
| 164.308(a)(6)(ii) | Phala Network performs a test of all components of the incident response plan and procedures at least annually through different mechanisms (e.g., walk-through or tabletop exercises, simulations, etc.). The documented plan and procedures are updated if necessary based on the results of the test. | Inspected the Incident Response Plan and latest Incident Response Test to determine that Phala Network performs a test of all components of the incident response plan and procedures at least annually through different mechanisms (e.g., walk-through or tabletop exercises, simulations, etc.). The documented plan and procedures are updated if necessary based on the results of the test. | No exceptions noted. |
| 164.308(a)(6)(ii) | Phala Network has an incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | Inspected the Incident Response Plan to determine that Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | No exceptions noted. |
| 164.308(a)(6)(ii) | Phala Network has incident management procedures that include detailed instructions on how to escalate a suspected incident to the Information Security Team and, when necessary, to the Privacy or Legal department. | Inspected the Incident Response Plan to determine that Phala Network has incident management procedures that include detailed instructions on how to escalate a suspected incident to the Information Security Team and, when necessary, to | Not tested. Control activity did not occur during the audit. |

| | | | |
|---|---|---|---|
| | Phala Network has a standard incident report template that must be completed for each incident. | the Privacy or Legal department. Phala Network has a standard incident report template that must be completed for each incident.<br><br>Inquired of company management to determine that no incidents occurred in the last year. | |
| 164.308(a)(7)(i) | Phala Network has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. | Inspected the Business Continuity Plan to determine that Phala Network has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. | No exceptions noted. |
| 164.308(a)(7)(i) | Phala Network performs a business impact analysis (BIA) periodically to identify criticality, business recovery order, and minimum service levels for key business processes and assets. Results of the business impact analysis are documented and incorporated into business continuity and disaster recovery plans. | Inspected the Business Continuity Plan and Business Impact Analysis to determine that Phala Network performs a business impact analysis (BIA) periodically to identify criticality, business recovery order, and minimum service levels for key business processes and assets. Results of the business impact analysis are documented and incorporated into business continuity and disaster recovery plans. | No exceptions noted. |
| 164.308(a)(7)(i) | Business-critical cloud resources are deployed in accordance with high availability architecture principles (e.g., replicated across multiple availability zones or regions, configured for high-availability, etc.). | Inspected the Backup Policy and availability zones to determine that business-critical cloud resources are deployed in accordance with high availability architecture principles (e.g., replicated across multiple availability zones or regions, configured for high-availability, etc.). | No exceptions noted. |
| 164.308(a)(7)(i) | Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | Inspected the Business Continuity Plan to determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | No exceptions noted. |
| 164.308(a)(7)(i) | Phala Network conducts tests of the business continuity/disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary. | Inspected the Business Continuity Plan and latest tabletop test to determine that Phala Network conducts tests of the business continuity/disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary. | No exceptions noted. |
| 164.308(a)(7)(ii)(A) | Backups are encrypted and segmented from production systems (e.g., air-gapped, replicated to a different region, stored offsite, etc.) to ensure protection from a disaster or incident. | Inspected the backup configurations and Backup Policy to determine that backups are encrypted and segmented from production systems (e.g., air-gapped, replicated to a different region, stored offsite, etc.) to ensure protection from a disaster or incident. | No exceptions noted. |
| 164.308(a)(7)(ii)(A) | Backups of production data are performed at least daily and are configured to be retained in accordance with the retention periods established in company policies and | Inspected backup configurations, the Phala Cloud Data Backup Procedure, and Backup Policy to determine that backups of production data are performed at least daily and are configured to be | No exceptions noted. |

| | | | |
|---|---|---|---|
| | procedures. | retained in accordance with the retention periods established in company policies and procedures. | |
| 164.308(a)(7)(ii)(A) | Phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | Inspected the Backup Policy to determine that phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | No exceptions noted. |
| 164.308(a)(7)(ii)(A) | Automated notifications are sent to personnel in the event of a backup failure. Backup failures are investigated and resolved by engineering personnel following company policies and procedures. | Inspected the backup configurations to determine that automated notifications are sent to personnel in the event of a backup failure. Backup failures are investigated and resolved by engineering personnel following company policies and procedures. | No exceptions noted. |
| 164.308(a)(7)(ii)(A) | Phala Network tests the integrity and recoverability of backed-up data at least annually. | Inspected the Backup Policy and Backup Restore Test History to determine that Phala Network tests the integrity and recoverability of backed-up data at least annually. | No exceptions noted. |
| 164.308(a)(7)(ii)(A) | Business-critical cloud resources are deployed in accordance with high availability architecture principles (e.g., replicated across multiple availability zones or regions, configured for high-availability, etc.). | Inspected the Backup Policy and availability zones to determine that business-critical cloud resources are deployed in accordance with high availability architecture principles (e.g., replicated across multiple availability zones or regions, configured for high-availability, etc.). | No exceptions noted. |
| 164.308(a)(7)(ii)(B) | Phala Network performs a business impact analysis (BIA) periodically to identify criticality, business recovery order, and minimum service levels for key business processes and assets. Results of the business impact analysis are documented and incorporated into business continuity and disaster recovery plans. | Inspected the Business Continuity Plan and Business Impact Analysis to determine that Phala Network performs a business impact analysis (BIA) periodically to identify criticality, business recovery order, and minimum service levels for key business processes and assets. Results of the business impact analysis are documented and incorporated into business continuity and disaster recovery plans. | No exceptions noted. |
| 164.308(a)(7)(ii)(B) | Phala Network has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. | Inspected the Business Continuity Plan to determine that Phala Network has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. | No exceptions noted. |
| 164.308(a)(7)(ii)(B) | Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | Inspected the Business Continuity Plan to determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | No exceptions noted. |
| 164.308(a)(7)(ii)(C) | Phala Network has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. | Inspected the Business Continuity Plan to determine that Phala Network has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.308(a)(7)(ii)(C) | Phala Network performs a business impact analysis (BIA) periodically to identify criticality, business recovery order, and minimum service levels for key business processes and assets. Results of the business impact analysis are documented and incorporated into business continuity and disaster recovery plans. | Inspected the Business Continuity Plan and Business Impact Analysis to determine that Phala Network performs a business impact analysis (BIA) periodically to identify criticality, business recovery order, and minimum service levels for key business processes and assets. Results of the business impact analysis are documented and incorporated into business continuity and disaster recovery plans. | No exceptions noted. |
| 164.308(a)(7)(ii)(C) | Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | Inspected the Business Continuity Plan to determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | No exceptions noted. |
| 164.308(a)(7)(ii)(D) | Phala Network conducts tests of the business continuity/disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary. | Inspected the Business Continuity Plan and latest tabletop test to determine that Phala Network conducts tests of the business continuity/disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary. | No exceptions noted. |
| 164.308(a)(7)(ii)(E) | Phala Network performs a business impact analysis (BIA) periodically to identify criticality, business recovery order, and minimum service levels for key business processes and assets. Results of the business impact analysis are documented and incorporated into business continuity and disaster recovery plans. | Inspected the Business Continuity Plan and Business Impact Analysis to determine that Phala Network performs a business impact analysis (BIA) periodically to identify criticality, business recovery order, and minimum service levels for key business processes and assets. Results of the business impact analysis are documented and incorporated into business continuity and disaster recovery plans. | No exceptions noted. |
| 164.308(a)(8) | Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | Inspected the Information Security Policy and company security policies to determine that Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | No exceptions noted. |
| 164.308(a)(8) | Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.). | Inspected the Information Security Policy to determine that management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.).<br><br>Inspected review and approval monitoring records to determine that management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | organizational risks, etc.). | |
| 164.308(a)(8) | Phala Network conducts risk assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented (e.g., in a risk register). | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network conducts risks assessments periodically as required by company policy and compliance requirements. The risk assessment includes consideration of threats and vulnerabilities and an evaluation of the likelihood and impact for each risk. A risk owner is assigned to each risk, and every risk is assigned a risk treatment option. Results of the risk assessment are documented (e.g., in a risk register). | No exceptions noted. |
| 164.308(a)(8) | The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed. | Inspected meeting minutes to determine that the company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed. | No exceptions noted. |
| 164.308(a)(8) | Production systems and resources are monitored and automated alerts are sent out to personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary. | Inspected the Datadog monitoring dashboard and Logging and Monitoring Policy to determine that production systems and resources are monitored and automated alerts are sent out personnel based on pre-configured rules. Events are triaged to determine if they constitute an incident and escalated per policy if necessary. | No exceptions noted. |
| 164.308(a)(8) | Phala Network performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. | Inspected the HIPAA framework dashboard to determine that Phala Network performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. | No exceptions noted. |
| 164.308(a)(8) | An external penetration test of production environments is performed by an independent third party periodically or after any significant infrastructure or application changes. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies. | Inspected the Vulnerability Management Policy and latest penetration test report to determine that an external penetration test of production environments is performed by an independent third party periodically or after any significant infrastructure or application changes. Results are reviewed by management and vulnerabilities are tracked to resolution in accordance with company policies. | No exceptions noted. |
| 164.308(b)(1) | Phala Network obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and Phala Network's requirements. Results of the review and action items, if any, are documented. | Inspected the Vendor Management Policy, vendor inventory, and compliance reports to determine that Phala Network obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and Phala Network's requirements. Results of | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | the review and action items, if any, are documented. | |
| 164.308(b)(1) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.308(b)(1) | Phala Network shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. | No exceptions noted. |
| 164.308(b)(1) | Phala Network requires its contractors to read and acknowledge the Code of Conduct, read and acknowledge the Acceptable Use Policy, and pass a background check. | Inspected the Code of Conduct to determine that Phala Network requires its contractors to read and acknowledge the Code of Conduct, read and acknowledge the Acceptable Use Policy, and pass a background check.<br><br>Inspected personnel compliance records to determine that Phala Network requires its contractors to read and acknowledge the Code of Conduct, read and acknowledge the Acceptable Use Policy, and pass a background check. | No exceptions noted. |
| 164.308(b)(3) | Phala Network shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. | No exceptions noted. |
| 164.310(a)(1) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.310(a)(1) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.310(a)(2)(i) | Business-critical cloud resources are deployed in accordance with high availability architecture | Inspected the Backup Policy and availability zones to determine that business-critical cloud resources | No exceptions noted. |

| | | | |
|---|---|---|---|
| | principles (e.g., replicated across multiple availability zones or regions, configured for high-availability, etc.). | are deployed in accordance with high availability architecture principles (e.g., replicated across multiple availability zones or regions, configured for high-availability, etc.). | |
| 164.310(a)(2)(i) | Phala Network has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. | Inspected the Business Continuity Plan to determine that Phala Network has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. | No exceptions noted. |
| 164.310(a)(2)(i) | Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | Inspected the Business Continuity Plan to determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | No exceptions noted. |
| 164.310(a)(2)(ii) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.310(a)(2)(ii) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.310(a)(2)(iii) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.310(a)(2)(iii) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.310(a)(2)(iv) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.310(b) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.310(b) | Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | Inspected the Information Security Policy and company security policies to determine that Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | No exceptions noted. |
| 164.310(b) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.310(b) | Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | Inspected the Acceptable Use Policy to determine that Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | No exceptions noted. |
| 164.310(c) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.310(c) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.310(d)(1) | Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | Inspected the Asset Management Policy to determine that Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | No exceptions noted. |
| 164.310(d)(2)(i) | Phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures. | Inspected the Data Protection Policy and Information Disposal Procedure to determine that phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.<br><br>Inquired of the company to determine that no hardware decommissioning events were needed in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.310(d)(2)(i) | Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | Inspected the Asset Management Policy to determine that Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | No exceptions noted. |
| 164.310(d)(2)(ii) | Phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures. | Inspected the Data Protection Policy and Information Disposal Procedure to determine that phala Network disposes of data on hardware through secure means, such as wiping and hard | Not tested. Control activity did not occur during the audit. |

| | | | |
|---|---|---|---|
| | | drive destruction, in accordance with documented policies and procedures.<br><br>Inquired of the company to determine that no hardware decommissioning events were needed in the last year. | |
| 164.310(d)(2)(ii) | Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | Inspected the Asset Management Policy to determine that Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | No exceptions noted. |
| 164.310(d)(2)(iii) | Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | Inspected the Asset Management Policy to determine that Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | No exceptions noted. |
| 164.310(d)(2)(iii) | A centralized asset register is maintained for physical, cloud, and other assets that includes descriptive attributes for asset accountability such as owner, description, location, classification, and/or other information based on the type of asset. Processes are in place to maintain an updated inventory through manual reviews (e.g., as a result of new purchases, installations, removals, system changes, etc.) or automated mechanisms. | Inspected the Asset Management Policy and Asset Inventory to determine that a centralized asset register is maintained for physical, cloud, and other assets that includes descriptive attributes for asset accountability such as owner, description, location, classification, and/or other information based on the type of asset. Processes are in place to maintain an updated inventory through manual reviews (e.g., as a result of new purchases, installations, removals, system changes, etc.) or automated mechanisms. | No exceptions noted. |
| 164.310(d)(2)(iv) | Automated notifications are sent to personnel in the event of a backup failure. Backup failures are investigated and resolved by engineering personnel following company policies and procedures. | Inspected the backup configurations to determine that automated notifications are sent to personnel in the event of a backup failure. Backup failures are investigated and resolved by engineering personnel following company policies and procedures. | No exceptions noted. |
| 164.310(d)(2)(iv) | Backups are encrypted and segmented from production systems (e.g., air-gapped, replicated to a different region, stored offsite, etc.) to ensure protection from a disaster or incident. | Inspected the backup configurations and Backup Policy to determine that backups are encrypted and segmented from production systems (e.g., air-gapped, replicated to a different region, stored offsite, etc.) to ensure protection from a disaster or incident. | No exceptions noted. |
| 164.310(d)(2)(iv) | Business-critical cloud resources are deployed in accordance with high availability architecture principles (e.g., replicated across multiple availability zones or regions, configured for high-availability, etc.). | Inspected the Backup Policy and availability zones to determine that business-critical cloud resources are deployed in accordance with high availability architecture principles (e.g., replicated across multiple availability zones or regions, configured for high-availability, etc.). | No exceptions noted. |
| 164.310(d)(2)(iv) | Phala Network tests the integrity and recoverability of backed-up data at least annually. | Inspected the Backup Policy and Backup Restore Test History to determine that Phala Network tests the integrity and recoverability of backed-up data at least annually. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.310(d)(2)(iv) | Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | Inspected the Business Continuity Plan to determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | No exceptions noted. |
| 164.310(d)(2)(iv) | Backups of production data are performed at least daily and are configured to be retained in accordance with the retention periods established in company policies and procedures. | Inspected backup configurations, the Phala Cloud Data Backup Procedure, and Backup Policy to determine that backups of production data are performed at least daily and are configured to be retained in accordance with the retention periods established in company policies and procedures. | No exceptions noted. |
| 164.310(d)(2)(iv) | Phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | Inspected the Backup Policy to determine that phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | No exceptions noted. |
| 164.312(a)(1) | Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | Inspected the System Access Control Policy and most recent Access Review records to determine that management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | No exceptions noted. |
| 164.312(a)(1) | Access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | Inspected the access provision register and System Access Control Policy to determine that access requests to information resources, including physical access and access to systems and data, are documented and approved by management based on least privilege, need to know, and segregation of duties principles. | No exceptions noted. |
| 164.312(a)(1) | Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | Inspected the System Access Control Policy to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.<br><br>Inspected access configurations and records from a recent access review to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | No exceptions noted. |
| 164.312(a)(1) | Phala Network uses a termination checklist to ensure that an employee's system access, including physical access, is removed within a | Inspected the System Access Control Policy and termination checklist to determine that Phala Network uses a termination checklist to ensure that | No exceptions noted. |

| | | | |
|---|---|---|---|
| | specified timeframe and all organization assets (physical or electronic) are properly returned. | an employee's system access, including physical access, is removed within a specified timeframe and all organization assets (physical or electronic) are properly returned. | |
| 164.312(a)(1) | Phala Network has an established key management process in place to support the organization's use of cryptographic techniques. | Inspected the Encryption Policy and company encryption in transit status to determine that Phala Network has an established key management process in place to support the organization's use of cryptographic techniques. | No exceptions noted. |
| 164.312(a)(1) | Network security controls are in place to restrict public access to remote server administration ports (e.g., SSH, RDP) to authorized IP addresses or address ranges only. | Inspected the Network Security Policy and network configurations to determine that network security controls are in place to restrict public access to remote server administration ports (e.g., SSH, RDP) to authorized IP addresses or address ranges only. | No exceptions noted. |
| 164.312(a)(1) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.312(a)(1) | System and physical access is revoked within one business day of the effective termination date for terminated users (including employees, third parties and vendors, and other personnel). | Inspected the System Access Control Policy to determine that System and physical access is revoked within one business day of effective termination date for terminated users (including employees, third parties and vendors, and other personnel).<br><br>Inspected revocation records within SLA to determine that terminated users must have access revoked within one business day. | No exceptions noted. |
| 164.312(a)(1) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.312(a)(1) | Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | Inspected the Access Control Policy to determine that Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.<br><br>Inspected the access review and user configurations to determine that administrative or privileged access to systems, resources, and functions is restricted to authorized personnel. | No exceptions noted. |
| 164.312(a)(2)(i) | Root password authentication to production resources (e.g., virtual machines, containers, etc.) is disabled and only allowed for under | Inspected the System Access Control Policy to determine that Root password authentication to production resources (e.g., virtual machines, | No exceptions noted. |

| | | | |
|---|---|---|---|
| | exceptional circumstances for a limited time duration based on documented business justification and approval from management. | containers, etc.) is disabled and only allowed for under exceptional circumstances for a limited time duration based on documented business justification and approval from management.<br><br>Inspected Root password disabled to determine that root password log in is not allowed. | |
| 164.312(a)(2)(i) | Authentication to systems requires the use of unique identities. | Inspected a list of employees to determine that authentication to systems requires the use of unique identities. | No exceptions noted. |
| 164.312(a)(2)(i) | Phala Network has implemented systems or mechanisms to centralize authentication and account management across the organization (e.g., directory service, identity provider, etc.). | Inspected the Data Protection Policy and MFA enforced organization wide through an SSO to determine that Phala Network has implemented systems or mechanisms to centralize authentication and account management across the organization (e.g., directory service, identity provider, etc.). | No exceptions noted. |
| 164.312(a)(2)(i) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.312(a)(2)(ii) | Phala Network conducts tests of the business continuity/disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary. | Inspected the Business Continuity Plan and latest tabletop test to determine that Phala Network conducts tests of the business continuity/disaster recovery plans at least annually. Results and lessons learned are documented, and updates to the plans are made as necessary. | No exceptions noted. |
| 164.312(a)(2)(ii) | Business-critical cloud resources are deployed in accordance with high availability architecture principles (e.g., replicated across multiple availability zones or regions, configured for high-availability, etc.). | Inspected the Backup Policy and availability zones to determine that business-critical cloud resources are deployed in accordance with high availability architecture principles (e.g., replicated across multiple availability zones or regions, configured for high-availability, etc.). | No exceptions noted. |
| 164.312(a)(2)(ii) | Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | Inspected the Business Continuity Plan to determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | No exceptions noted. |
| 164.312(a)(2)(ii) | Phala Network performs a business impact analysis (BIA) periodically to identify criticality, business recovery order, and minimum service levels for key business processes and assets. Results of the business impact analysis are documented and incorporated into business continuity and disaster recovery plans. | Inspected the Business Continuity Plan and Business Impact Analysis to determine that Phala Network performs a business impact analysis (BIA) periodically to identify criticality, business recovery order, and minimum service levels for key business processes and assets. Results of the business impact analysis are documented and incorporated into business continuity and disaster recovery plans. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.312(a)(2)(ii) | Phala Network has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. | Inspected the Business Continuity Plan to determine that Phala Network has a defined business continuity plan that outlines strategies for maintaining operations during a disruption. | No exceptions noted. |
| 164.312(a)(2)(iii) | Company-managed devices are configured to enforce a screensaver lock after a defined period of inactivity in accordance with company policies and compliance requirements. | Inspected the System Access Control Policy to determine that the company-managed devices are configured to enforce a screensaver lock after a defined period of inactivity in accordance with company policies and compliance requirements.<br><br>Inspected a list of personnel with screensaver lock enabled to determine that company-managed devices are configured to enforce a screensaver lock after a defined period of inactivity in accordance with company policies and compliance requirements. | No exceptions noted. |
| 164.312(a)(2)(iii) | Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | Inspected the Password Policy and password configurations in place to determine that Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | No exceptions noted. |
| 164.312(a)(2)(iii) | Phala Network's systems automatically terminate a user's logical session based on predefined conditions (e.g., predefined periods of inactivity, closure of the system or internet browser, etc.). | Inspected the System Access Control Policy and application logoff configuration to determine that Phala Network's systems automatically terminate a user's logical session based on predefined conditions (e.g., predefined periods of inactivity, closure of the system or internet browser, etc.). | No exceptions noted. |
| 164.312(a)(2)(iv) | Administrator access to web-based management interfaces is encrypted with strong cryptographic algorithms. | Inspected the Data Protection Policy and SSL certificate to determine that administrator access to web-based management interfaces is encrypted with strong cryptographic algorithms. | No exceptions noted. |
| 164.312(a)(2)(iv) | Hard-disk encryption is enabled on all company-managed devices. | Inspected the Data Protection Policy and disk encryption enabled status to determine that hard-disk encryption is enabled on all company-managed devices. | No exceptions noted. |
| 164.312(a)(2)(iv) | Data at rest is encrypted using strong cryptographic algorithms. | Inspected the data at rest encryption enabled status to determine that data at rest is encrypted using strong cryptographic algorithms. | No exceptions noted. |
| 164.312(a)(2)(iv) | Phala Network has an established key management process in place to support the organization's use of cryptographic techniques. | Inspected the Encryption Policy and company encryption in transit status to determine that Phala Network has an established key management process in place to support the organization's use of cryptographic techniques. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.312(a)(2)(iv) | Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | No exceptions noted. |
| 164.312(a)(2)(iv) | Data in transit is encrypted using strong cryptographic algorithms. | Inspected the Encryption Policy and SSL monitoring records to determine that data in transit is encrypted using strong cryptographic algorithms. | No exceptions noted. |
| 164.312(a)(2)(iv) | Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | Inspected the VPN enabled status, SSL status, and Encryption Policy to determine that remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | No exceptions noted. |
| 164.312(a)(2)(iv) | Phala Network has implemented data leakage prevention mechanisms to systems that could process, store or transmit sensitive information (e.g., sending personal information via email). These mechanisms are configured to prevent data leakage and generate audit logs and alerts. | Inspected the Data Protection Policy and Data Loss Prevention (DLP) Mechanism in place to determine that Phala Network has implemented data leakage prevention mechanisms to systems that could process, store or transmit sensitive information (e.g., sending personal information via email). These mechanisms are configured to prevent data leakage and generate audit logs and alerts. | No exceptions noted. |
| 164.312(b) | Phala Network has implemented tools to monitor Phala Network's messaging queues and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | Inspected the Logging and Monitoring Policy and messaging queue monitoring enabled status to determine that Phala Network has implemented tools to monitor Phala Network's messaging queues and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | No exceptions noted. |
| 164.312(b) | Backups are encrypted and segmented from production systems (e.g., air-gapped, replicated to a different region, stored offsite, etc.) to ensure protection from a disaster or incident. | Inspected the backup configurations and Backup Policy to determine that backups are encrypted and segmented from production systems (e.g., air-gapped, replicated to a different region, stored offsite, etc.) to ensure protection from a disaster or incident. | No exceptions noted. |
| 164.312(b) | Phala Network uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner. | Inspected the Datadog monitoring dashboard to determine that Phala Network uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner. | No exceptions noted. |
| 164.312(b) | A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary. | Inspected the AWS GuardDuty dashboard, WAF configured, and Logging and Monitoring Policy to determine that a threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.312(b) | Phala Network has implemented tools to monitor Phala Network's databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | Inspected the Logging and Monitoring Policy and Datadog monitoring dashboard to determine that Phala Network has implemented tools to monitor Phala Network's databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | No exceptions noted. |
| 164.312(b) | Phala Network has implemented tools to monitor Phala Network's servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | Inspected the Datadog monitoring dashboard and Logging and Monitoring Policy to determine that Phala Network has implemented tools to monitor Phala Network's servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | No exceptions noted. |
| 164.312(b) | Phala Network has implemented tools to monitor Phala Network's NoSQL databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | Inspected the Logging and Monitoring Policy and Datadog monitoring dashboard to determine that Phala Network has implemented tools to monitor Phala Network's databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | No exceptions noted. |
| 164.312(b) | Phala Network uses compliance automation software to identify, select, and continuously monitor internal controls. | Inspected the compliance platform dashboard to determine that Phala Network uses compliance automation software to identify, select, and continuously monitor internal controls. | No exceptions noted. |
| 164.312(b) | Phala Network has a defined plan for event logging that establishes the required criteria for logs, protection of logged information, and clock synchronization. | Inspected the Logging and Monitoring Policy, access review records, and clock synchronization configurations to determine that Phala Network has a defined plan for event logging that establishes the required criteria for logs, protection of logged information, and clock synchronization. | No exceptions noted. |
| 164.312(b) | Phala Network uses a centralized system that collects and stores logs of system activity and sends alerts to personnel based on pre-configured rules. Access to logs is restricted to authorized personnel. | Inspected the Datadog monitoring dashboard and Logging and Monitoring Policy to determine that Phala Network uses a centralized system that collects and stores logs of system activity and sends alerts to personnel based on pre-configured rules. Access to logs is restricted to authorized personnel. | No exceptions noted. |
| 164.312(c)(1) | Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | No exceptions noted. |
| 164.312(c)(1) | Phala Network ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with. | Inspected the company's layered integrity assurance process to determine that Phala Network ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.312(c)(1) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.312(c)(1) | Phala Network has implemented systems or mechanisms to centralize authentication and account management across the organization (e.g., directory service, identity provider, etc.). | Inspected the Data Protection Policy and MFA enforced organization wide through an SSO to determine that Phala Network has implemented systems or mechanisms to centralize authentication and account management across the organization (e.g., directory service, identity provider, etc.). | No exceptions noted. |
| 164.312(c)(2) | Phala Network has implemented tools to monitor Phala Network's messaging queues and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | Inspected the Logging and Monitoring Policy and messaging queue monitoring enabled status to determine that Phala Network has implemented tools to monitor Phala Network's messaging queues and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | No exceptions noted. |
| 164.312(c)(2) | Phala Network has implemented tools to monitor Phala Network's NoSQL databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | Inspected the Logging and Monitoring Policy and Datadog monitoring dashboard to determine that Phala Network has implemented tools to monitor Phala Network's databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | No exceptions noted. |
| 164.312(c)(2) | Phala Network has a defined plan for event logging that establishes the required criteria for logs, protection of logged information, and clock synchronization. | Inspected the Logging and Monitoring Policy, access review records, and clock synchronization configurations to determine that Phala Network has a defined plan for event logging that establishes the required criteria for logs, protection of logged information, and clock synchronization. | No exceptions noted. |
| 164.312(c)(2) | Phala Network has implemented tools to monitor Phala Network's servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | Inspected the Datadog monitoring dashboard and Logging and Monitoring Policy to determine that Phala Network has implemented tools to monitor Phala Network's servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | No exceptions noted. |
| 164.312(c)(2) | Phala Network uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner. | Inspected the Datadog monitoring dashboard to determine that Phala Network uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner. | No exceptions noted. |
| 164.312(c)(2) | Backups are encrypted and segmented from production systems (e.g., air-gapped, replicated to a different region, stored offsite, etc.) to | Inspected the backup configurations and Backup Policy to determine that backups are encrypted and segmented from production systems (e.g., | No exceptions noted. |

| | | | |
|---|---|---|---|
| | ensure protection from a disaster or incident. | air-gapped, replicated to a different region, stored offsite, etc.) to ensure protection from a disaster or incident. | |
| 164.312(c)(2) | Phala Network uses a centralized system that collects and stores logs of system activity and sends alerts to personnel based on pre-configured rules. Access to logs is restricted to authorized personnel. | Inspected the Datadog monitoring dashboard and Logging and Monitoring Policy to determine that Phala Network uses a centralized system that collects and stores logs of system activity and sends alerts to personnel based on pre-configured rules. Access to logs is restricted to authorized personnel. | No exceptions noted. |
| 164.312(c)(2) | Phala Network has implemented tools to monitor Phala Network's databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | Inspected the Logging and Monitoring Policy and Datadog monitoring dashboard to determine that Phala Network has implemented tools to monitor Phala Network's databases and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy. | No exceptions noted. |
| 164.312(c)(2) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.312(c)(2) | Phala Network ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with. | Inspected the company's layered integrity assurance process to determine that Phala Network ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with. | No exceptions noted. |
| 164.312(c)(2) | A threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary. | Inspected the AWS GuardDuty dashboard, WAF configured, and Logging and Monitoring Policy to determine that a threat detection system is in place to monitor web traffic and suspicious activity. When anomalous traffic activity is identified, alerts are automatically sent to personnel, investigated, and escalated through the incident management process, if necessary. | No exceptions noted. |
| 164.312(c)(2) | Phala Network uses compliance automation software to identify, select, and continuously monitor internal controls. | Inspected the compliance platform dashboard to determine that Phala Network uses compliance automation software to identify, select, and continuously monitor internal controls. | No exceptions noted. |
| 164.312(d) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.312(e)(1) | Phala Network has a documented policy that establishes requirements for the use of | Inspected the Encryption Policy to determine that Phala Network has a documented policy that | No exceptions noted. |

| | | | |
|---|---|---|---|
| | cryptographic controls. | establishes requirements for the use of cryptographic controls. | |
| 164.312(e)(1) | Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | Inspected the VPN enabled status, SSL status, and Encryption Policy to determine that remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | No exceptions noted. |
| 164.312(e)(1) | Network security controls are in place to restrict public access to remote server administration ports (e.g., SSH, RDP) to authorized IP addresses or address ranges only. | Inspected the Network Security Policy and network configurations to determine that network security controls are in place to restrict public access to remote server administration ports (e.g., SSH, RDP) to authorized IP addresses or address ranges only. | No exceptions noted. |
| 164.312(e)(1) | Data in transit is encrypted using strong cryptographic algorithms. | Inspected the Encryption Policy and SSL monitoring records to determine that data in transit is encrypted using strong cryptographic algorithms. | No exceptions noted. |
| 164.312(e)(1) | Administrator access to web-based management interfaces is encrypted with strong cryptographic algorithms. | Inspected the Data Protection Policy and SSL certificate to determine that administrator access to web-based management interfaces is encrypted with strong cryptographic algorithms. | No exceptions noted. |
| 164.312(e)(1) | Phala Network has implemented data leakage prevention mechanisms to systems that could process, store or transmit sensitive information (e.g., sending personal information via email). These mechanisms are configured to prevent data leakage and generate audit logs and alerts. | Inspected the Data Protection Policy and Data Loss Prevention (DLP) Mechanism in place to determine that Phala Network has implemented data leakage prevention mechanisms to systems that could process, store or transmit sensitive information (e.g., sending personal information via email). These mechanisms are configured to prevent data leakage and generate audit logs and alerts. | No exceptions noted. |
| 164.312(e)(2)(i) | Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | No exceptions noted. |
| 164.312(e)(2)(i) | Phala Network has implemented systems or mechanisms to centralize authentication and account management across the organization (e.g., directory service, identity provider, etc.). | Inspected the Data Protection Policy and MFA enforced organization wide through an SSO to determine that Phala Network has implemented systems or mechanisms to centralize authentication and account management across the organization (e.g., directory service, identity provider, etc.). | No exceptions noted. |
| 164.312(e)(2)(i) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.312(e)(2)(ii) | Phala Network has a documented policy that | Inspected the Encryption Policy to determine that | No exceptions noted. |

| | | | |
|---|---|---|---|
| | establishes requirements for the use of cryptographic controls. | Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | |
| 164.312(e)(2)(ii) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.312(e)(2)(ii) | Data at rest is encrypted using strong cryptographic algorithms. | Inspected the data at rest encryption enabled status to determine that data at rest is encrypted using strong cryptographic algorithms. | No exceptions noted. |
| 164.314(a)(1) | Phala Network obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and Phala Network's requirements. Results of the review and action items, if any, are documented. | Inspected the Vendor Management Policy, vendor inventory, and compliance reports to determine that Phala Network obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and Phala Network's requirements. Results of the review and action items, if any, are documented. | No exceptions noted. |
| 164.314(a)(1) | Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII | Inspected the Vendor Management Policy and vendor inventory to determine that Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII. | No exceptions noted. |
| 164.314(a)(1) | Phala Network requires vendors and third parties with access to personal information to sign a formal contract that requires them to notify Phala Network in the event of actual or suspected unauthorized disclosures of personal information | Inspected the Vendor Management Policy and a DPA to determine that Phala Network requires vendors and third parties with access to personal information to sign a formal contract that requires them to notify Phala Network in the event of actual or suspected unauthorized disclosures of personal information | No exceptions noted. |
| 164.314(a)(1) | Phala Network maintains a vendor/third party register that includes a complete and accurate list of vendors/third parties, relationship owners, description for each of the services provided, risk ratings, results of vendor/third party risk management activities, etc. Phala Network executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. | Inspected the Vendor Management Policy and Vendor Register to determine that Phala Network maintains a vendor/third party register that includes a complete and accurate list of vendors/third parties, relationship owners, description for each of the services provided, risk ratings, results of vendor/third party risk management activities, etc. Phala Network executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. | No exceptions noted. |
| 164.314(a)(1) | Phala Network shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing | Inspected the Vendor Management Policy and a DPA to determine that Phala Network shares information with vendors and third parties only when an executed agreement (e.g., service | No exceptions noted. |

| | | | |
|---|---|---|---|
| | agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. | agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. | |
| 164.314(a)(1) | Phala Network provides vendors and third parties with information on how to report breaches to Phala Network. | Inspected the Breach Notification Policy, Privacy Policy, and a DPA to determine that Phala Network provides vendors and third parties with information on how to report breaches to Phala Network. | No exceptions noted. |
| 164.314(a)(1) | Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | Inspected the Data Processing Agreement and Vendor Management Policy to determine that Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | No exceptions noted. |
| 164.314(a)(1) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.314(a)(1) | Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | No exceptions noted. |
| 164.314(a)(1) | Phala Network has a defined policy that establishes the requirements related to Business Associate Agreements | Inspected the Business Associate Policy to determine that phala Network has a defined policy that establishes the requirements related to Business Associate Agreements. | No exceptions noted. |
| 164.314(a)(2)(i)(A) | Phala Network shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. | No exceptions noted. |
| 164.314(a)(2)(i)(A) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | entire life cycle. | |
| 164.314(a)(2)(i)(A) | Phala Network maintains a vendor/third party register that includes a complete and accurate list of vendors/third parties, relationship owners, description for each of the services provided, risk ratings, results of vendor/third party risk management activities, etc. Phala Network executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. | Inspected the Vendor Management Policy and Vendor Register to determine that Phala Network maintains a vendor/third party register that includes a complete and accurate list of vendors/third parties, relationship owners, description for each of the services provided, risk ratings, results of vendor/third party risk management activities, etc. Phala Network executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. | No exceptions noted. |
| 164.314(a)(2)(i)(A) | Phala Network has a defined policy that establishes the requirements related to Business Associate Agreements | Inspected the Business Associate Policy to determine that phala Network has a defined policy that establishes the requirements related to Business Associate Agreements. | No exceptions noted. |
| 164.314(a)(2)(i)(A) | Phala Network provides vendors and third parties with information on how to report breaches to Phala Network. | Inspected the Breach Notification Policy, Privacy Policy, and a DPA to determine that Phala Network provides vendors and third parties with information on how to report breaches to Phala Network. | No exceptions noted. |
| 164.314(a)(2)(i)(A) | Phala Network obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and Phala Network's requirements. Results of the review and action items, if any, are documented. | Inspected the Vendor Management Policy, vendor inventory, and compliance reports to determine that Phala Network obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and Phala Network's requirements. Results of the review and action items, if any, are documented. | No exceptions noted. |
| 164.314(a)(2)(i)(A) | Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | No exceptions noted. |
| 164.314(a)(2)(i)(A) | Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII | Inspected the Vendor Management Policy and vendor inventory to determine that Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII. | No exceptions noted. |
| 164.314(a)(2)(i)(A) | Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or | Inspected the Data Processing Agreement and Vendor Management Policy to determine that Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a | No exceptions noted. |

| | | | |
|---|---|---|---|
| | other specific instructions or requirements. | manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | |
| 164.314(a)(2)(i)(A) | Phala Network requires vendors and third parties with access to personal information to sign a formal contract that requires them to notify Phala Network in the event of actual or suspected unauthorized disclosures of personal information | Inspected the Vendor Management Policy and a DPA to determine that Phala Network requires vendors and third parties with access to personal information to sign a formal contract that requires them to notify Phala Network in the event of actual or suspected unauthorized disclosures of personal information | No exceptions noted. |
| 164.314(a)(2)(i)(B) | Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | No exceptions noted. |
| 164.314(a)(2)(i)(B) | Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII | Inspected the Vendor Management Policy and vendor inventory to determine that Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII. | No exceptions noted. |
| 164.314(a)(2)(i)(B) | Phala Network has a defined policy that establishes the requirements related to Business Associate Agreements | Inspected the Business Associate Policy to determine that phala Network has a defined policy that establishes the requirements related to Business Associate Agreements. | No exceptions noted. |
| 164.314(a)(2)(i)(B) | Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | Inspected the Data Processing Agreement and Vendor Management Policy to determine that Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | No exceptions noted. |
| 164.314(a)(2)(i)(B) | Phala Network obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and Phala Network's requirements. Results of the review and action items, if any, are documented. | Inspected the Vendor Management Policy, vendor inventory, and compliance reports to determine that Phala Network obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and Phala Network's requirements. Results of the review and action items, if any, are documented. | No exceptions noted. |
| 164.314(a)(2)(i)(B) | Phala Network shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing | Inspected the Vendor Management Policy and a DPA to determine that Phala Network shares information with vendors and third parties only when an executed agreement (e.g., service | No exceptions noted. |

| | | | |
|---|---|---|---|
| | agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. | agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. | |
| 164.314(a)(2)(i)(B) | Phala Network maintains a vendor/third party register that includes a complete and accurate list of vendors/third parties, relationship owners, description for each of the services provided, risk ratings, results of vendor/third party risk management activities, etc. Phala Network executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. | Inspected the Vendor Management Policy and Vendor Register to determine that Phala Network maintains a vendor/third party register that includes a complete and accurate list of vendors/third parties, relationship owners, description for each of the services provided, risk ratings, results of vendor/third party risk management activities, etc. Phala Network executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. | No exceptions noted. |
| 164.314(a)(2)(i)(B) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.314(a)(2)(i)(B) | Phala Network provides vendors and third parties with information on how to report breaches to Phala Network. | Inspected the Breach Notification Policy, Privacy Policy, and a DPA to determine that Phala Network provides vendors and third parties with information on how to report breaches to Phala Network. | No exceptions noted. |
| 164.314(a)(2)(i)(B) | Phala Network requires vendors and third parties with access to personal information to sign a formal contract that requires them to notify Phala Network in the event of actual or suspected unauthorized disclosures of personal information | Inspected the Vendor Management Policy and a DPA to determine that Phala Network requires vendors and third parties with access to personal information to sign a formal contract that requires them to notify Phala Network in the event of actual or suspected unauthorized disclosures of personal information | No exceptions noted. |
| 164.314(a)(2)(i)(C) | Phala Network maintains a vendor/third party register that includes a complete and accurate list of vendors/third parties, relationship owners, description for each of the services provided, risk ratings, results of vendor/third party risk management activities, etc. Phala Network executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. | Inspected the Vendor Management Policy and Vendor Register to determine that Phala Network maintains a vendor/third party register that includes a complete and accurate list of vendors/third parties, relationship owners, description for each of the services provided, risk ratings, results of vendor/third party risk management activities, etc. Phala Network executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. | No exceptions noted. |
| 164.314(a)(2)(i)(C) | Phala Network has a defined policy that establishes the requirements related to Business Associate Agreements | Inspected the Business Associate Policy to determine that phala Network has a defined policy that establishes the requirements related to | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | Business Associate Agreements. | |
| 164.314(a)(2)(i)(C) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.314(a)(2)(i)(C) | Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | No exceptions noted. |
| 164.314(a)(2)(i)(C) | Phala Network requires vendors and third parties with access to personal information to sign a formal contract that requires them to notify Phala Network in the event of actual or suspected unauthorized disclosures of personal information | Inspected the Vendor Management Policy and a DPA to determine that Phala Network requires vendors and third parties with access to personal information to sign a formal contract that requires them to notify Phala Network in the event of actual or suspected unauthorized disclosures of personal information | No exceptions noted. |
| 164.314(a)(2)(i)(C) | Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | Inspected the Data Processing Agreement and Vendor Management Policy to determine that Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | No exceptions noted. |
| 164.314(a)(2)(i)(C) | Phala Network provides vendors and third parties with information on how to report breaches to Phala Network. | Inspected the Breach Notification Policy, Privacy Policy, and a DPA to determine that Phala Network provides vendors and third parties with information on how to report breaches to Phala Network. | No exceptions noted. |
| 164.314(a)(2)(i)(C) | Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII | Inspected the Vendor Management Policy and vendor inventory to determine that Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII. | No exceptions noted. |
| 164.314(a)(2)(i)(C) | Phala Network shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network shares information with vendors and third parties only when an executed agreement (e.g., service agreements, business associate agreements, data processing agreements, etc.) is in place that includes security, confidentiality, and privacy requirements for the transfer and processing of information. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.314(a)(2)(i)(C) | Phala Network obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and Phala Network's requirements. Results of the review and action items, if any, are documented. | Inspected the Vendor Management Policy, vendor inventory, and compliance reports to determine that Phala Network obtains and reviews compliance reports or other evidence for critical vendors and service providers at least annually to monitor the third parties' compliance with industry frameworks, regulations, standards (e.g., SOC 2, ISO, PCI DSS, etc.) and Phala Network's requirements. Results of the review and action items, if any, are documented. | No exceptions noted. |
| 164.314(a)(2)(ii) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.314(a)(2)(ii) | Phala Network maintains a vendor/third party register that includes a complete and accurate list of vendors/third parties, relationship owners, description for each of the services provided, risk ratings, results of vendor/third party risk management activities, etc. Phala Network executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. | Inspected the Vendor Management Policy and Vendor Register to determine that Phala Network maintains a vendor/third party register that includes a complete and accurate list of vendors/third parties, relationship owners, description for each of the services provided, risk ratings, results of vendor/third party risk management activities, etc. Phala Network executes agreements with vendors and service providers involved in accessing, processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. | No exceptions noted. |
| 164.314(a)(2)(ii) | Phala Network has a defined policy that establishes the requirements related to Business Associate Agreements | Inspected the Business Associate Policy to determine that phala Network has a defined policy that establishes the requirements related to Business Associate Agreements. | No exceptions noted. |
| 164.314(a)(2)(iii) | Phala Network has a defined policy that establishes the requirements related to Business Associate Agreements | Inspected the Business Associate Policy to determine that phala Network has a defined policy that establishes the requirements related to Business Associate Agreements. | No exceptions noted. |
| 164.314(a)(2)(iii) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.314(a)(2)(iii) | Phala Network maintains a vendor/third party register that includes a complete and accurate list of vendors/third parties, relationship owners, description for each of the services provided, risk ratings, results of vendor/third party risk management activities, etc. Phala Network executes agreements with vendors and service providers involved in accessing, processing, storing or managing information | Inspected the Vendor Management Policy and Vendor Register to determine that Phala Network maintains a vendor/third party register that includes a complete and accurate list of vendors/third parties, relationship owners, description for each of the services provided, risk ratings, results of vendor/third party risk management activities, etc. Phala Network executes agreements with vendors and service providers involved in accessing, | No exceptions noted. |

| | | | |
|---|---|---|---|
| | assets that outline the responsibilities of each vendor or service provider. | processing, storing or managing information assets that outline the responsibilities of each vendor or service provider. | |
| 164.314(b)(1) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.314(b)(2)(i) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.314(b)(2)(ii) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.314(b)(2)(iii) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.314(b)(2)(iv) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.316(a) | Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | Inspected the Vulnerability Management Policy to determine that Phala Network has a defined policy that establishes requirements for vulnerability management across the organization, including monitoring, cataloging, and assigning risk ratings to vulnerabilities to prioritize remediation efforts. | No exceptions noted. |
| 164.316(a) | Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | Inspected the System Access Control Policy to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege.<br><br>Inspected access configurations and records from a recent access review to determine that Phala Network authorizes access to information resources, including data and the systems that store or process sensitive data, based on the principle of least privilege. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.316(a) | Phala Network has an incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | Inspected the Incident Response Plan to determine that Phala Network has a documented incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | No exceptions noted. |
| 164.316(a) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.316(a) | Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors. | Inspected the Acceptable Use Policy and Data Protection Policy to determine that Phala Network Management has approved all policies that detail how customer data may be made accessible and should be handled. These policies are accessible to all employees and contractors.<br><br>Inspected acknowledgement records to determine that these policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.316(a) | Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has a documented policy that establishes requirements for the use of cryptographic controls. | No exceptions noted. |
| 164.316(a) | Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | Inspected the Vendor Management Policy and a DPA to determine that Phala Network's privacy policies or other specific instructions for handling personal information, including requirements and procedures to notify Phala Network of breaches or unauthorized disclosures, are communicated to third parties to whom personal information is disclosed. | No exceptions noted. |
| 164.316(a) | Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | Inspected the Physical Security Policy and approval records to determine that Phala Network has security policies that have been approved by management and detail how physical access to the company's headquarters is maintained. These policies are accessible to all employees and contractors. | No exceptions noted. |
| 164.316(a) | Phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | Inspected the Backup Policy to determine that phala Network has defined and documented a backup policy that establishes the requirements for backup information, software and systems. | No exceptions noted. |
| 164.316(a) | Phala Network communicates to customers | Inspected the Data Processing Agreement to | No exceptions noted. |

| | | | |
|---|---|---|---|
| | any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Phala Network obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.). | determine that Phala Network communicates to customers any use of subprocessors to process PII (e.g., through a list of subprocessors in the company website or data processing agreement, etc.). Phala Network obtains authorization from customers for the use of subprocessors (e.g., through executed data processing agreements, accepting the terms in the website, etc.).. | |
| 164.316(a) | Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | Inspected the Asset Management Policy to determine that Phala Network has established and documented a policy that outlines requirements for the management and tracking of company assets. | No exceptions noted. |
| 164.316(a) | Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | Inspected the Information Security Policy and company security policies to determine that Phala Network has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control. | No exceptions noted. |
| 164.316(a) | Phala Network communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Phala Network provides notification to relevant parties of any changes to service commitments and system requirements. | Inspected the Terms and Conditions of Use including update records, and a services agreement to determine that Phala Network communicates service commitments and system requirements to customers and other external parties, as appropriate, through contracts, agreements, company website, etc. Phala Network provides notification to relevant parties of any changes to service commitments and system requirements. | No exceptions noted. |
| 164.316(a) | Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | Inspected the Business Continuity Plan to determine that Phala Network has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario. | No exceptions noted. |
| 164.316(a) | Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures. | Inspected the Incident Response Plan to determine that Phala Network evaluates security events to determine if they constitute an incident. Incidents are assigned a priority, categorized, documented, tracked, escalated, contained, eradicated, communicated, and resolved in accordance with company policies and procedures.<br><br>Inquired of company management to determine that no security incidents occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.316(a) | Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | Inspected the Software Development Life Cycle Policy to determine that Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | deployment. | |
| 164.316(a) | Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected the Information Security Policy and Incident Response Plan to determine that Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | No exceptions noted. |
| 164.316(a) | The security team communicates important information security events to company management in a timely manner. | Inspected the Incident Response Plan and internal channel for security events communication to determine that the security team communicates important information security events to company management in a timely manner. | No exceptions noted. |
| 164.316(a) | Phala Network has documented policies and procedures for erasure or destruction of information that has been identified for disposal. | Inspected the Information Disposal Procedure to determine that Phala Network has documented policies and procedures for erasure or destruction of information that has been identified for disposal. | No exceptions noted. |
| 164.316(a) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.316(a) | Phala Network maintains policies and procedures that define allowable use and disclosure scenarios. | Inspected the Data Protection Policy to determine that Phala Network maintains policies and procedures that define allowable use and disclosure scenarios. | No exceptions noted. |
| 164.316(a) | Phala Network has an established policy and procedures that governs the use of cryptographic controls. | Inspected the Encryption Policy to determine that Phala Network has an established policy and procedures that governs the use of cryptographic controls. | No exceptions noted. |
| 164.316(a) | Phala Network communicates its Privacy Policy on its public-facing website. | Inspected the public privacy policy to determine that Phala Network communicates its Privacy Policy on its public-facing website. | No exceptions noted. |
| 164.316(a) | Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | Inspected the Acceptable Use Policy to determine that Phala Network has a documented acceptable use policy that outlines requirements for personnel's usage of company assets. | No exceptions noted. |
| 164.316(a) | Management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | Inspected the Information Security Management System Plan to determine that management has defined and documented roles and responsibilities for implementation and oversight of the risk management and compliance programs (e.g., security, privacy, AI, etc.). | No exceptions noted. |
| 164.316(a) | Phala Network maintains a documented code | Inspected the Code of Conduct to determine that | No exceptions noted. |

| | | | |
|---|---|---|---|
| | of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter.<br><br>Inspected acknowledgement records to determine that Phala Network maintains a documented code of conduct. Eligible personnel are required to acknowledge Phala Network's code of conduct during onboarding and annually thereafter. | |
| 164.316(a) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.316(a) | Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | Inspected the Information Security Policy and training completion records to determine that Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | No exceptions noted. |
| 164.316(a) | Phala Network maintains a publicly available privacy policy/notice. | Inspected the public privacy policy to determine that Phala Network maintains a publicly available privacy policy/notice. | No exceptions noted. |
| 164.316(a) | Anti-malware software is installed on all company-managed devices. | Inspected the anti-malware enabled status on workstations to determine that anti-malware software is installed on all company-managed devices. | No exceptions noted. |
| 164.316(a) | Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | Inspected the Data Retention Policy to determine that Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | No exceptions noted. |
| 164.316(a) | Phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures. | Inspected the Data Protection Policy and Information Disposal Procedure to determine that phala Network disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.<br><br>Inquired of the company to determine that no hardware decommissioning events were needed in the last year. | Not tested. Control activity did not occur during the audit. |

| | | | |
|---|---|---|---|
| 164.316(a) | Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | Inspected the Password Policy and password configurations in place to determine that Phala Network has a documented policy outlining the minimum requirements for passwords used for authentication to organizational systems. Password requirements are enforced for all systems in accordance with company policy. | No exceptions noted. |
| 164.316(a) | Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | Inspected the Data Classification Policy to determine that Phala Network has established a data classification policy in order to identify the types of information stored or processed by the organization and the protection measures that are required for each. | No exceptions noted. |
| 164.316(a) | Phala Network has a documented policy that outlines requirements for physical security. | Inspected the Physical Security policy to determine that Phala Network has a documented policy that outlines requirements for physical security. | No exceptions noted. |
| 164.316(a) | Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | Inspected the VPN enabled status, SSL status, and Encryption Policy to determine that remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.) | No exceptions noted. |
| 164.316(a) | Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | Inspected the Risk Assessment Policy and Risk Assessment to determine that Phala Network has defined and documented a process for risk assessment and risk management that outlines the organization's approach for identifying risks and assigning risk owners, the risk acceptance criteria, and the approach for evaluating and treating risks based on the defined criteria. | No exceptions noted. |
| 164.316(a) | Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | Inspected the Acceptable Use Policy to determine that Phala Network has defined clear desk and clear screen policies and procedures to protect confidential data (physical and electronic) which are communicated to personnel and enforced across the organization. | No exceptions noted. |
| 164.316(b)(1)(i) | The security team communicates important information security events to company management in a timely manner. | Inspected the Incident Response Plan and internal channel for security events communication to determine that the security team communicates important information security events to company management in a timely manner. | No exceptions noted. |
| 164.316(b)(1)(i) | Phala Network's management reviews the privacy notice to ensure that the privacy notice is accurate. | Inspected the Phala Cloud Annual Privacy Policy Review Report to determine that Phala Network's management reviews the privacy notice to ensure that the privacy notice is accurate.<br><br>Inspected the Privacy Policy which includes a last updated date to determine that Phala Network's | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | management reviews the privacy notice to ensure that the privacy notice is accurate. | |
| 164.316(b)(1)(i) | Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected the Information Security Policy and Incident Response Plan to determine that Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | No exceptions noted. |
| 164.316(b)(1)(i) | Phala Network's management reviews the online privacy policy and/or notice at least annually to validate its continued suitability and accuracy. The online privacy policy/notice includes the date it was last updated. Phala Network notifies customers of changes to the privacy notice and the nature of the changes, including when personal information will be used for new purposes not previously identified. | Inspected the Phala Cloud Annual Privacy Policy Review Report and Privacy Policy to determine that Phala Network's management reviews the online privacy policy and/or notice at least annually to validate its continued suitability and accuracy. The online privacy policy/notice includes the date it was last updated. Phala Network notifies customers of changes to the privacy notice and the nature of the changes, including when personal information will be used for new purposes not previously identified. | No exceptions noted. |
| 164.316(b)(1)(i) | Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.). | Inspected the Information Security Policy to determine that management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.).<br><br>Inspected review and approval monitoring records to determine that management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.). | No exceptions noted. |
| 164.316(b)(1)(i) | Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | Inspected the System Access Control Policy and most recent Access Review records to determine that management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | No exceptions noted. |
| 164.316(b)(1)(i) | Executive management meets on a quarterly basis to review compliance with privacy practices and privacy regulations. | Inspected the company's Information Security Management System Plan and formalized review documentation to determine that executive management meets on a quarterly basis to review compliance with privacy practices and privacy regulations. | Exceptions noted. |

| | | | |
|---|---|---|---|
| | | Inquired of the company to determine that quarterly privacy practices and privacy regulation reviews were conducted but not formally documented and evidence of quarterly reviews isn't available. | |
| 164.316(b)(1)(i) | A documented network diagram is in place to document system boundaries and connections to external networks. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment. | Inspected the network diagram including review date to determine that a documented network diagram is in place to document system boundaries and connections to external networks. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment. | No exceptions noted. |
| 164.316(b)(1)(i) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.316(b)(1)(ii) | Phala Network's management reviews the privacy notice to ensure that the privacy notice is accurate. | Inspected the Phala Cloud Annual Privacy Policy Review Report to determine that Phala Network's management reviews the privacy notice to ensure that the privacy notice is accurate.<br><br>Inspected the Privacy Policy which includes a last updated date to determine that Phala Network's management reviews the privacy notice to ensure that the privacy notice is accurate. | No exceptions noted. |
| 164.316(b)(1)(ii) | Management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | Inspected the System Access Control Policy and most recent Access Review records to determine that management performs user access reviews periodically (as defined by policy and compliance requirements) to validate user accounts, including third party or vendor accounts, and their associated privileges remain appropriate. The review includes validation of logical and physical access as necessary. Changes resulting from the review, if any, are documented and implemented. | No exceptions noted. |
| 164.316(b)(1)(ii) | Executive management meets on a quarterly basis to review compliance with privacy practices and privacy regulations. | Inspected the company's Information Security Management System Plan and formalized review documentation to determine that executive management meets on a quarterly basis to review compliance with privacy practices and privacy regulations.<br><br>Inquired of the company to determine that quarterly privacy practices and privacy regulation reviews were conducted but not formally documented and evidence of quarterly reviews isn't available. | Exceptions noted. |
| 164.316(b)(1)(ii) | Management reviews and approves company policies at least annually. Updates to the | Inspected the Information Security Policy to determine that management reviews and approves | No exceptions noted. |

| | | | |
|---|---|---|---|
| | policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.). | company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.).<br><br>Inspected review and approval monitoring records to determine that management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.). | |
| 164.316(b)(1)(ii) | Phala Network has developed and documented a policy that outlines requirements for access control. | Inspected the System Access Control Policy to determine that Phala Network has developed and documented a policy that outlines requirements for access control. | No exceptions noted. |
| 164.316(b)(1)(ii) | The security team communicates important information security events to company management in a timely manner. | Inspected the Incident Response Plan and internal channel for security events communication to determine that the security team communicates important information security events to company management in a timely manner. | No exceptions noted. |
| 164.316(b)(1)(ii) | Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected the Information Security Policy and Incident Response Plan to determine that Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | No exceptions noted. |
| 164.316(b)(1)(ii) | A documented network diagram is in place to document system boundaries and connections to external networks. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment. | Inspected the network diagram including review date to determine that a documented network diagram is in place to document system boundaries and connections to external networks. The diagram is reviewed and approved by management at least annually and updated as necessary when there are changes to the environment. | No exceptions noted. |
| 164.316(b)(1)(ii) | Phala Network's management reviews the online privacy policy and/or notice at least annually to validate its continued suitability and accuracy. The online privacy policy/notice includes the date it was last updated. Phala Network notifies customers of changes to the privacy notice and the nature of the changes, including when personal information will be used for new purposes not previously identified. | Inspected the Phala Cloud Annual Privacy Policy Review Report and Privacy Policy to determine that Phala Network's management reviews the online privacy policy and/or notice at least annually to validate its continued suitability and accuracy. The online privacy policy/notice includes the date it was last updated. Phala Network notifies customers of changes to the privacy notice and the nature of the changes, including when personal information will be used for new purposes not previously identified. | No exceptions noted. |
| 164.316(b)(2)(i) | Phala Network retains HIPAA-related policies and procedures for at least 6 years from the date of the document's creation or when it was | Inspected the maintained policy version history to determine that Phala Network retains HIPAA-related policies and procedures for at least 6 years from | No exceptions noted. |

| | | | |
|---|---|---|---|
| | last in effect (whichever is later). | the date of the document's creation or when it was last in effect (whichever is later). | |
| 164.316(b)(2)(i) | Phala Network disposes of customer data upon termination of services in accordance with contractual agreements. | Inspected the Data Retention Policy, customer data deletion dashboard, and status to determine that Phala Network disposes of customer data upon termination of services in accordance with contractual agreements. | No exceptions noted. |
| 164.316(b)(2)(i) | Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | Inspected the Data Retention Policy to determine that Phala Network has a documented and implemented a policy for data retention defining the types of data (including company and customer data) and the period of time for which they should be retained. | No exceptions noted. |
| 164.316(b)(2)(i) | Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | Inspected the Data Protection Policy to determine that Phala Network has a documented policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data. | No exceptions noted. |
| 164.316(b)(2)(ii) | Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | Inspected the Information Security Policy and Incident Response Plan to determine that Phala Network has an assigned security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines. | No exceptions noted. |
| 164.316(b)(2)(ii) | The security team communicates important information security events to company management in a timely manner. | Inspected the Incident Response Plan and internal channel for security events communication to determine that the security team communicates important information security events to company management in a timely manner. | No exceptions noted. |
| 164.316(b)(2)(iii) | Management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.). | Inspected the Information Security Policy to determine that management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.).<br><br>Inspected review and approval monitoring records to determine that management reviews and approves company policies at least annually. Updates to the policies are made as deemed necessary (e.g., based on changes to business objectives, legal or regulatory requirements, organizational risks, etc.). | No exceptions noted. |
| 164.402 | Phala Network has an incident response plan that outlines roles, responsibilities, and procedures to document, analyze, categorize, | Inspected the Incident Response Plan to determine that Phala Network has a documented incident response plan that outlines roles, responsibilities, | No exceptions noted. |

| | | | |
|---|---|---|---|
| | and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | and procedures to document, analyze, categorize, and respond to incidents. The incident response plan reviewed periodically and updated as needed according to lessons learned from previous incidents and industry developments. | |
| 164.402 | Phala Network provides vendors and third parties with information on how to report breaches to Phala Network. | Inspected the Breach Notification Policy, Privacy Policy, and a DPA to determine that Phala Network provides vendors and third parties with information on how to report breaches to Phala Network. | No exceptions noted. |
| 164.402 | Phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations. | Inspected the Incident Response Plan and Breach Notification Policy to determine that phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.<br><br>Inquired of company management to determine that no incidents or breaches occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.402 | Internal communication channels are in place for employees to report failures, events, incidents, policy violations, concerns, and other issues to company management, including anonymous reporting channels if applicable. | Inspected internal report channel to determine that internal communication channels are in place for employees to report failures, events, incidents, policy violations, concerns, and other issues to company management, including anonymous reporting channels if applicable. | No exceptions noted. |
| 164.402 | Phala Network provides external communication mechanisms for customers and third parties (e.g., communication features, support portal, external ticketing system, etc.) to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs. | Inspected the contact information page, contact information in the Privacy Policy, and communication ticket performance dashboard to determine that Phala Network provides external communication mechanisms for customers and third parties (e.g., communication features, support portal, external ticketing system, etc.) to report complaints, failures, bugs, incidents, vulnerabilities, requests for information, etc. Customer communications are responded to within defined SLAs. | No exceptions noted. |
| 164.402 | Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | Inspected the Information security policy, a DPA, and Breach Notification Policy to determine that Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | No exceptions noted. |
| 164.402 | Phala Network has established training | Inspected the Information Security Policy and | No exceptions noted. |

| | | | |
|---|---|---|---|
| | programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | training completion records to determine that Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | |
| 164.404(a) | Phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations. | Inspected the Incident Response Plan and Breach Notification Policy to determine that phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.<br><br>Inquired of company management to determine that no incidents or breaches occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.404(a) | Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | Inspected the Information security policy, a DPA, and Breach Notification Policy to determine that Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | No exceptions noted. |
| 164.404(b) | Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | Inspected the Information security policy, a DPA, and Breach Notification Policy to determine that Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | No exceptions noted. |
| 164.404(b) | Phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations. | Inspected the Incident Response Plan and Breach Notification Policy to determine that phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.<br><br>Inquired of company management to determine that no incidents or breaches occurred in the last | Not tested. Control activity did not occur during the audit. |

| | | | |
|---|---|---|---|
| | | year. | |
| 164.404(c) | Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | Inspected the Information security policy, a DPA, and Breach Notification Policy to determine that Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | No exceptions noted. |
| 164.404(c) | Phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations. | Inspected the Incident Response Plan and Breach Notification Policy to determine that phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.<br><br>Inquired of company management to determine that no incidents or breaches occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.404(d) | Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | Inspected the Information security policy, a DPA, and Breach Notification Policy to determine that Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | No exceptions noted. |
| 164.404(d) | Phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations. | Inspected the Incident Response Plan and Breach Notification Policy to determine that phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.<br><br>Inquired of company management to determine that no incidents or breaches occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.406 | Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor | Inspected the Information security policy, a DPA, and Breach Notification Policy to determine that Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the | No exceptions noted. |

| | | | |
|---|---|---|---|
| | and its clients (cloud service customers). | contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | |
| 164.406 | Phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations. | Inspected the Incident Response Plan and Breach Notification Policy to determine that phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.<br><br>Inquired of company management to determine that no incidents or breaches occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.408 | Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | Inspected the Information security policy, a DPA, and Breach Notification Policy to determine that Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | No exceptions noted. |
| 164.408 | Phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations. | Inspected the Incident Response Plan and Breach Notification Policy to determine that phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.<br><br>Inquired of company management to determine that no incidents or breaches occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.41 | Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | Inspected the Information security policy, a DPA, and Breach Notification Policy to determine that Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | No exceptions noted. |
| 164.41 | Phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in | Inspected the Incident Response Plan and Breach Notification Policy to determine that phala Network provides communications about breaches and incidents to affected parties, organizational | Not tested. Control activity did not occur during the audit. |

| | | | |
|---|---|---|---|
| | accordance with company policies and procedures and contractual and legal obligations. | officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.<br><br>Inquired of company management to determine that no incidents or breaches occurred in the last year. | |
| 164.412 | Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | Inspected the Information security policy, a DPA, and Breach Notification Policy to determine that Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | No exceptions noted. |
| 164.412 | Phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations. | Inspected the Incident Response Plan and Breach Notification Policy to determine that phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.<br><br>Inquired of company management to determine that no incidents or breaches occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.414(a) | Phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations. | Inspected the Incident Response Plan and Breach Notification Policy to determine that phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.<br><br>Inquired of company management to determine that no incidents or breaches occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.414(a) | Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | Inspected the Information security policy, a DPA, and Breach Notification Policy to determine that Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.414(b) | Phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations. | Inspected the Incident Response Plan and Breach Notification Policy to determine that phala Network provides communications about breaches and incidents to affected parties, organizational officials, authorities, and other internal and external stakeholders, in accordance with company policies and procedures and contractual and legal obligations.<br><br>Inquired of company management to determine that no incidents or breaches occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.414(b) | Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | Inspected the Information security policy, a DPA, and Breach Notification Policy to determine that Phala Network information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers). | No exceptions noted. |
| 164.502(a)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(a)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(a)(3) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(a)(4) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(a)(5)(i) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(a)(5)(ii) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.502(b)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(b)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(c) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(d)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(d)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(e) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(f) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(g) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(h) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(i) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.502(j)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | requirements of the HIPAA Privacy Rule. | |
| 164.502(j)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.504(e) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.504(e) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.504(f) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.504(f) | Phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | Inspected the Vendor Management Policy to determine that phala Network has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle. | No exceptions noted. |
| 164.504(g) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.506 | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.506(a) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.506(b) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.508(a) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.508(b) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.508(b)(3) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.508(b)(4) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.508(c) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.510(a) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.510(a)(3) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.510(b)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.510(b)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.510(b)(3) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.510(b)(4) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.510(b)(5) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | requirements of the HIPAA Privacy Rule. | |
| 164.512(a) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(b) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(c) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(d) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(e) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(f)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(f)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(f)(3) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(f)(4) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(f)(5) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(f)(6) | Phala Network has a defined policy that | Inspected the Privacy, Use, and Disclosure Policy | No exceptions noted. |

| | | | |
|---|---|---|---|
| | establishes the requirements of the HIPAA Privacy Rule | and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | |
| 164.512(g) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(h) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(i)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(i)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(j) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(k)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(k)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(k)(3) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(k)(4) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(k)(5) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.512(k)(6) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.512(l) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.514(a) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.514(d) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.514(d)(3) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.514(d)(4) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.514(d)(5) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.514(e) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.514(f) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.514(g) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.514(h) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | requirements of the HIPAA Privacy Rule. | |
| 164.520(a) | Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | Inspected the privacy policy and public website where consent is required to determine that Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | No exceptions noted. |
| 164.520(a) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.520(b) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.520(b) | Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | Inspected the privacy policy and public website where consent is required to determine that Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | No exceptions noted. |
| 164.520(c)(1) | Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | Inspected the privacy policy and public website where consent is required to determine that Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | No exceptions noted. |
| 164.520(c)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.520(c)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.520(c)(2) | Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | Inspected the privacy policy and public website where consent is required to determine that Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | No exceptions noted. |
| 164.520(c)(3) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | requirements of the HIPAA Privacy Rule. | |
| 164.520(c)(3) | Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | Inspected the privacy policy and public website where consent is required to determine that Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | No exceptions noted. |
| 164.520(d) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.520(d) | Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | Inspected the privacy policy and public website where consent is required to determine that Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | No exceptions noted. |
| 164.520(e) | Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | Inspected the privacy policy and public website where consent is required to determine that Phala Network provides notice of its privacy practices to users prior to accessing the system. Users are required to explicitly acknowledge the privacy policy prior to entering information into the system. | No exceptions noted. |
| 164.520(e) | Phala Network retains HIPAA-related policies and procedures for at least 6 years from the date of the document's creation or when it was last in effect (whichever is later). | Inspected the maintained policy version history to determine that Phala Network retains HIPAA-related policies and procedures for at least 6 years from the date of the document's creation or when it was last in effect (whichever is later). | No exceptions noted. |
| 164.520(e) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.522(a)(1) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.522(a)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.522(a)(1) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.522(a)(2) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.522(a)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.522(a)(2) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.522(a)(3) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.522(a)(3) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.522(a)(3) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.522(a)(3) | Phala Network retains HIPAA-related policies and procedures for at least 6 years from the date of the document's creation or when it was last in effect (whichever is later). | Inspected the maintained policy version history to determine that Phala Network retains HIPAA-related policies and procedures for at least 6 years from the date of the document's creation or when it was last in effect (whichever is later). | No exceptions noted. |
| 164.522(b) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.522(b) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.522(b) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.524(a)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala | No exceptions noted. |

| | | | |
|---|---|---|---|
| | Privacy Rule | Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | |
| 164.524(a)(1) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.524(a)(1) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.524(a)(2) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.524(a)(2) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.524(a)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.524(a)(3) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.524(a)(3) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.524(a)(3) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.524(a)(4) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.524(a)(4) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.524(a)(4) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.524(b) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.524(b) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.524(b) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.524(c) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.524(c) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.524(c) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.524(d)(1) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.524(d)(1) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.524(d)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.524(d)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.524(d)(2) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.524(d)(2) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.524(d)(3) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.524(d)(3) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.524(d)(3) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.524(d)(4) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.524(d)(4) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.524(d)(4) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.524(e) | Users can access all of their personal information through the application by navigating to their settings and profile. | Inspected users profile section to determine that users can access their personal information through the application by navigating to their settings and profile. | No exceptions noted. |
| 164.524(e) | Users accessing their personal information through Phala Network's application must be authenticated with a username and password. | Inspected login page to determine that users can access their personal information through the application must be authenticated. | No exceptions noted. |
| 164.524(e) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | requirements of the HIPAA Privacy Rule. | |
| 164.526(a)(1) | Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | Inspected users profile section to determine that Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | No exceptions noted. |
| 164.526(a)(1) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.526(a)(1) | Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the businessÃ¢â‚¬â„¢s response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements. | Inspected the privacy inquiry tracking process to determine that Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the business' response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements.<br><br>Inquired of company management to determine that no privacy rights requests occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.526(a)(2) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.526(a)(2) | Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | Inspected users profile section to determine that Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | No exceptions noted. |
| 164.526(a)(2) | Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the businessÃ¢â‚¬â„¢s response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements. | Inspected the privacy inquiry tracking process to determine that Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the business' response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements.<br><br>Inquired of company management to determine that no privacy rights requests occurred in the last | Not tested. Control activity did not occur during the audit. |

| | | | |
|---|---|---|---|
| | | year. | |
| 164.526(b) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.526(b) | Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | Inspected users profile section to determine that Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | No exceptions noted. |
| 164.526(b) | Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the businessÃ¢â‚¬â„¢s response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements. | Inspected the privacy inquiry tracking process to determine that Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the business' response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements.<br><br>Inquired of company management to determine that no privacy rights requests occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.526(c) | Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the businessÃ¢â‚¬â„¢s response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements. | Inspected the privacy inquiry tracking process to determine that Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the business' response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements.<br><br>Inquired of company management to determine that no privacy rights requests occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.526(c) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.526(c) | Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | Inspected users profile section to determine that Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their | No exceptions noted. |

| | | | |
|---|---|---|---|
| | | profile settings. | |
| 164.526(d) | Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | Inspected users profile section to determine that Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | No exceptions noted. |
| 164.526(d) | Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the businessÃ¢â‚¬â„¢s response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements. | Inspected the privacy inquiry tracking process to determine that Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the business' response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements.<br><br>Inquired of company management to determine that no privacy rights requests occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.526(d) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.526(e) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.526(e) | Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | Inspected users profile section to determine that Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | No exceptions noted. |
| 164.526(e) | Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the businessÃ¢â‚¬â„¢s response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements. | Inspected the privacy inquiry tracking process to determine that Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the business' response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements.<br><br>Inquired of company management to determine that no privacy rights requests occurred in the last | Not tested. Control activity did not occur during the audit. |

| | | | |
|---|---|---|---|
| | | year. | |
| 164.526(f) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.526(f) | Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | Inspected users profile section to determine that Phala Network provides a mechanism for users to view, correct, and/or delete their personal information by authenticating into the system with a username and password and navigating to their profile settings. | No exceptions noted. |
| 164.526(f) | Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the businessÃ¢â‚¬â„¢s response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements. | Inspected the privacy inquiry tracking process to determine that Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the business' response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements.<br><br>Inquired of company management to determine that no privacy rights requests occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.528(a) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.528(a) | Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII | Inspected the Vendor Management Policy and vendor inventory to determine that Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII. | No exceptions noted. |
| 164.528(a) | Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | Inspected the Data Processing Agreement and Vendor Management Policy to determine that Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | No exceptions noted. |
| 164.528(b) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |

| | | | |
|---|---|---|---|
| 164.528(b) | Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII | Inspected the Vendor Management Policy and vendor inventory to determine that Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII. | No exceptions noted. |
| 164.528(b) | Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | Inspected the Data Processing Agreement and Vendor Management Policy to determine that Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | No exceptions noted. |
| 164.528(c) | Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | Inspected the Data Processing Agreement and Vendor Management Policy to determine that Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | No exceptions noted. |
| 164.528(c) | Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII | Inspected the Vendor Management Policy and vendor inventory to determine that Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII. | No exceptions noted. |
| 164.528(c) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.528(d) | Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII | Inspected the Vendor Management Policy and vendor inventory to determine that Phala Network maintains a documented list of third parties and vendors that are authorized to receive or access PII. | No exceptions noted. |
| 164.528(d) | Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | Inspected the Data Processing Agreement and Vendor Management Policy to determine that Phala Network discloses personal information only to third parties who have agreements with Phala Network to protect personal information in a manner consistent with the relevant aspects of Phala Network's privacy notice or other specific instructions or requirements. | No exceptions noted. |
| 164.528(d) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.530(a) | Phala Network has formally assigned | Inspected the Information Security Policy to | No exceptions noted. |

| | | | |
|---|---|---|---|
| | responsibility for information security in the organization to a Chief Information Security Officer or other security-knowledgeable member of management. | determine that Phala Network has formally assigned responsibility for information security in the organization to a Chief Information Security Officer or other security-knowledgeable member of management. | |
| 164.530(a) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.530(b) | Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | Inspected the Information Security Policy and training completion records to determine that Phala Network has established training programs to help personnel gain awareness of information security best practices. Personnel (including employees and contractors as applicable) are required to complete the training during onboarding. Periodic refresher training is provided to personnel at least annually and as deemed necessary (e.g., upon changes in security requirements, policies, regulations, etc.). | No exceptions noted. |
| 164.530(b) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.530(b) | Phala Network has established a training program for the use and disclosure of protected health information (PHI) to help personnel understand their obligations and responsibilities related to HIPAA. All eligible members of the workforce are required to complete this training during onboarding and annually thereafter. | Inspected the PHI training completion status to determine that Phala Network has established a training program for the use and disclosure of protected health information (PHI) to help personnel understand their obligations and responsibilities related to HIPAA. All eligible members of the workforce are required to complete this training during onboarding and annually thereafter. | No exceptions noted. |
| 164.530(c) | Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | Inspected the Software Development Life Cycle Policy to determine that Phala Network has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment. | No exceptions noted. |
| 164.530(d)(1) | Phala Network provides a contact mechanism for data subjects to submit privacy-related requests or report privacy incidents (e.g., email address, customer portal, etc.). | Inspected DPA, Privacy Policy, and public contact information to determine that Phala Network provides a contact mechanism for data subjects to submit privacy-related requests or report privacy incidents (e.g., email address, customer portal, etc.). | No exceptions noted. |
| 164.530(d)(1) | Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, | Inspected the privacy inquiry tracking process to determine that Phala Network maintains records of privacy rights requests in ticket or log format that | Not tested. Control activity did not occur during the audit. |

| | | | |
|---|---|---|---|
| | manner in which the request was made, the date of the businessÃ¢â‚¬â„¢s response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements. | includes the date of request, nature of request, manner in which the request was made, the date of the business' response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements.<br><br>Inquired of company management to determine that no privacy rights requests occurred in the last year. | |
| 164.530(d)(1) | Phala Network informs users about how to contact Phala Network with inquiries, complaints, and disputes via the privacy practices that are posted on the Phala Network's public-facing website. | Inspected contact portal on the company's public website and Privacy Policy to determine that Phala Network informs users about how to contact Phala Network with inquiries, complaints, and disputes via the privacy practices that are posted on the Phala Network's public-facing website. | No exceptions noted. |
| 164.530(d)(2) | Phala Network provides a contact mechanism for data subjects to submit privacy-related requests or report privacy incidents (e.g., email address, customer portal, etc.). | Inspected DPA, Privacy Policy, and public contact information to determine that Phala Network provides a contact mechanism for data subjects to submit privacy-related requests or report privacy incidents (e.g., email address, customer portal, etc.). | No exceptions noted. |
| 164.530(d)(2) | Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the businessÃ¢â‚¬â„¢s response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements. | Inspected the privacy inquiry tracking process to determine that Phala Network maintains records of privacy rights requests in ticket or log format that includes the date of request, nature of request, manner in which the request was made, the date of the business' response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. Records are retained for a defined period in accordance with legal requirements.<br><br>Inquired of company management to determine that no privacy rights requests occurred in the last year. | Not tested. Control activity did not occur during the audit. |
| 164.530(d)(2) | Phala Network informs users about how to contact Phala Network with inquiries, complaints, and disputes via the privacy practices that are posted on the Phala Network's public-facing website. | Inspected contact portal on the company's public website and Privacy Policy to determine that Phala Network informs users about how to contact Phala Network with inquiries, complaints, and disputes via the privacy practices that are posted on the Phala Network's public-facing website. | No exceptions noted. |
| 164.530(e) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.530(f) | Phala Network has a defined policy that | Inspected the Privacy, Use, and Disclosure Policy | No exceptions noted. |

| | | | |
|---|---|---|---|
| | establishes the requirements of the HIPAA Privacy Rule | and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | |
| 164.530(g) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.530(h) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.530(i) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.530(j) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.530(j) | Phala Network retains HIPAA-related policies and procedures for at least 6 years from the date of the document's creation or when it was last in effect (whichever is later). | Inspected the maintained policy version history to determine that Phala Network retains HIPAA-related policies and procedures for at least 6 years from the date of the document's creation or when it was last in effect (whichever is later). | No exceptions noted. |
| 164.530(k) | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |
| 164.532 | Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule | Inspected the Privacy, Use, and Disclosure Policy and related documentation to determine that Phala Network has a defined policy that establishes the requirements of the HIPAA Privacy Rule. | No exceptions noted. |

# Other Information Provided by Hashforest Technology LLC

The information in this section is presented by the Company to provide additional information to its user entities, business partners, and other specified parties and is not part of the Company's description of its system and controls included in the System Scope and Purpose section and the Procedures Performed and Findings section. The evidence has not been subjected to the procedures applied in the examination of the description of Hashforest Technology LLC and the suitability of the design of controls to achieve the Company's service commitments and system requirements based on the applicable criteria, and accordingly, Prescient Security LLC expresses no opinion on it.

## Management's Response to the exception at 164.306(e), 164.316(b)(1)(i), and 164.316(b)(1)(ii)

**Control Description:** Executive management meets on a quarterly basis to review compliance with privacy practices and privacy regulations.

**Exception noted:** Inquired of the company to determine that quarterly privacy practices and privacy regulation reviews were conducted but not formally documented and evidence of quarterly reviews isn't available.

**Management's Response:** Management acknowledges the exception. During the audit period, executive reviews of the company's privacy practices and applicable privacy regulations took place on an informal basis within the team's regular meetings; they were not consistently documented, and contemporaneous minutes evidencing each quarterly review were not retained. Management has not created any backdated records for the audit period and presents this gap transparently.

To remediate the finding and prevent recurrence, management has formally established a recurring quarterly Compliance and Privacy Review, chaired by the CEO with the CTO and Head of Operations as required attendees, operating on a fixed cadence (Q1 in April, Q2 in July, Q3 in October, Q4 in January), with the first formal session held immediately following the audit closeout. The standing agenda covers security and privacy incidents, the risk register, user access reviews, policy changes, sub-processors and vendor status, Drata framework readiness, and data subject requests. Minutes for each session are reviewed and approved by the participants and retained in the Compliance Reviews repository per the Data Retention Policy (minimum six years for HIPAA-relevant records, consistent with 45 CFR §164.316(b)(2) and §164.530(j)).

Accountability for convening the review, recording minutes, and retaining evidence is assigned to the Head of Security and Compliance. Supporting documentation: HIPAA-RFE-2026-09 Quarterly Compliance Review (provided in the Drata Audit Hub).

PHALA

Hashforest Technology LLC

Prescient Security LLC
1900 Church Street, Suite 300
Nashville, TN 37203

June 29, 2026

In connection with your engagement to report on Hashforest Technology LLC's compliance with the HIPAA Security, Privacy, and Breach Notification Rules, we confirm, to the best of our knowledge and belief, as of June 5, 2026, the date of your report, the following representations made to you during your examination:

1) We have disclosed to you all known matters that may contradict the presentation of the evidence or the suitability of the design of the controls.

2) We have disclosed to you any communications from regulatory agencies, user entities, or others received through the date of this letter affecting the presentation of the description or the suitability of the design of the controls.

3) We are responsible for determining the scope of your examination, including identifying the time period covered by the engagement, services that are the subject of the examination, the system providing the services (including boundaries of the system), and risks relevant to business partners who provide intellectual property or services related to the system.

4) We are responsible for identifying and analyzing the risks that threaten the achievement of HIPAA compliance with the Security, Privacy, and Breach Notification Rules.

5) We are responsible for designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that we comply with HIPAA Security, Privacy, and Breach Notification Rules.

6) We have provided you with the following:

   a) All relevant information and access, as agreed upon in the terms of the engagement, to all information such as records, documentation, service-level agreements, and internal audit or other reports, of which we are aware that is relevant to your examination and our assertion.

   b) Access to additional information you have requested from us for the purpose of the engagement.

   c) Unrestricted access to persons within the appropriate parties from whom you determined was necessary to obtain evidence relevant to your engagement.

7) We have disclosed to you any known events subsequent to the date of the engagement letter up to the date of this letter that would have a material effect on the suitability of the design or operating effectiveness of the controls.

8) We have disclosed to you any instances of noncompliance with laws and regulations, fraud, or uncorrected misstatements attributable to the service organization that are not clearly trivial and that may affect one or more user entities, and whether such incidents have been communicated appropriately to affected user entities.

9) We have disclosed to you any actual, suspected, or alleged fraud or noncompliance with laws or regulations that could adversely affect the description of the service organization's system, the suitability of the design of the controls stated therein, or achievement of its service commitments and system requirements.

10) We also have disclosed to you all instances about which we are aware of the following:

    a) Misstatements and omissions in the description.

    b) Instances in which controls have not been suitably designed or implemented as described.

    c) Instances in which controls did not operate effectively or as described.

11) We have disclosed to you all identified system incidents that resulted in a significant impairment of the service organization's compliance with the HIPAA Security, Privacy, and Breach Notification Rules as of June 5, 2026.

12) We have disclosed to you any changes in the controls that are likely to be relevant to report users occurring through the date of this letter.

13) We have responded fully to all inquiries made to us by you during the examination.

14) We understand that your report is intended solely for the use and information of management of the organization and others within the organization, user entities to which we provide services, and other specified parties who have sufficient knowledge and understanding to consider it, along with other information, if any. We intend to distribute your report only to those specified parties.

15) We understand this engagement does not represent a legal determination.

We understand that your examination was conducted in accordance with audit standards established by the ISO 19011 standard and was designed for the purpose of expressing an opinion about whether, in all material respects, the controls stated were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable standard. We also understand that the opinion was based on your examination and that the procedures performed in the examination were limited to those that you considered necessary.

签署人：
Xudong Guo
9A78B0FB3B59451...
Name

Head of Operations
Title