SOC 2 Type 1 Report

Hashforest Technology LLC

Restricted Use & Distribution

Report Issue Date: December 19, 2025

A Type 1 Independent Service Auditor's Report on Controls Relevant to Security

AUDIT AND ATTESTATION BY

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

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

Table of Contents

PRESCIENT ASSURANCE

SECTION 1

Management's Assertion

PHALA

Management's Assertion

We have prepared the accompanying description of Hashforest Technology LLC's system as of October 01, 2025, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report *(With Revised Implementation Guidance—2022)*. The description is intended to provide report users with information about Hashforest Technology LLC's system that may be useful when assessing the risks arising from interactions with Hashforest Technology LLC's system, particularly information about system controls that Hashforest Technology LLC has designed to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*.

Hashforest Technology LLC uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls at Hashforest Technology LLC, to achieve Hashforest Technology LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Hashforest Technology LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Hashforest Technology LLC's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at Hashforest Technology LLC, to achieve Hashforest Technology LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Hashforest Technology LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Hashforest Technology LLC's controls.

We confirm, to the best of our knowledge and belief, that:

1. The description presents Hashforest Technology LLC's system that was designed and implemented as of October 01, 2025 in accordance with the description criteria.
2. The controls stated in the description were suitably designed as of October 01, 2025, to provide reasonable assurance that Hashforest Technology LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Hashforest Technology LLC's controls as of that date.

Lin Tong
CEO of Hashforest Technology
Hashforest Technology LLC

PRESCIENT ASSURANCE

SECTION 2

Independent Service Auditor's Report

Independent Service Auditor's Report

To: Hashforest Technology LLC

Scope

We have examined Hashforest Technology LLC's accompanying description of its system as of October 01, 2025, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report *(With Revised Implementation Guidance—2022),* and the suitability of the design of controls stated in the description as of October 01, 2025, to provide reasonable assurance that Hashforest Technology LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022).*

Hashforest Technology LLC uses a subservice organization for cloud hosting services services and provides application maintenance and support. The description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls at Hashforest Technology LLC, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Hashforest Technology LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Hashforest Technology LLC's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed are necessary, along with controls at Hashforest Technology LLC, to achieve Hashforest Technology LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Hashforest Technology LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Hashforest Technology LLC's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design of such controls.

Service Organization's Responsibilities

Hashforest Technology LLC is responsible for its service commitments and system requirements and for designing effective controls within the system to provide reasonable assurance that Hashforest Technology LLC's service commitments and system requirements were achieved. In Section 1, Hashforest Technology LLC has provided the accompanying assertion titled "Management's Assertion of Hashforest Technology LLC" (assertion) about the description and the suitability of design of controls stated therein. Hashforest Technology LLC is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design of controls involves the following:

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
4. Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
5. Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature and timing of those tests are listed in section IV.

Opinion

In our opinion, in all material respects:

1. The description presents Hashforest Technology LLC's system that was designed and implemented as of October 01, 2025 in accordance with the description criteria.
2. The controls stated in the description were suitably designed as of October 01, 2025, to provide reasonable assurance that Hashforest Technology LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Hashforest Technology LLC's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Hashforest Technology LLC, user entities of Hashforest Technology LLC's system as of October 01, 2025, 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:

1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.

3. Internal control and its limitations.
4. Complementary subservice organization controls and Complementary User Entity organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. The risks that may threaten the achievement of the service 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.

Prescient Assurance

Prescient Assurance LLC
Nashville, TN
December 18, 2025

PRESCIENT ASSURANCE

SECTION 3

System Description

PHALA

DC 1: 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 organizations 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.

DC 2: 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.

DC 3: The Components of the System Used to Provide the Services

3.1 Infrastructure & Network Architecture

Application/ System	Process/ Transaction	Purchased or Developed	Platform and Operating System	Data Type
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

3.2 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.

3.3 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

3.3.1 Physical Security

Hashforest Technology LLC's production servers are maintained by Phala Clouds 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 trusted infrastructure providers such as OVH and DCML. The compute infrastructure combines CPU nodes and GPU clusters supporting IntelTrust Domain Extensions (TDX) and NVIDIA Confidential Compute to ensure hardware-level isolation and data protection during processing. All infrastructure is operated under strict physical and logical access controls, while auxiliary services including global DNS, CDN, and DDoS protection are provided by Cloudflare.. 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 Phala Clouds 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 trusted infrastructure providers such as OVH and DCML. The compute infrastructure combines CPU nodes and GPU clusters supporting Intel Trust Domain Extensions (TDX) and NVIDIA Confidential Compute to ensure hardware-level isolation and data protection during processing. All infrastructure is operated under strict physical and logical access controls, while auxiliary services including global DNS, CDN, and DDoS protection are provided by Cloudflare. on at least an annual basis.

3.3.2 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 provision access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Hashforest Technology LLC's policies, completing security training. These steps must be completed within Within 3 business days of hire. All new employees are required to review Phala Clouds Security, Privacy, and Acceptable Use Policies and complete mandatory security awareness training within three business days of onboarding. days of hire.

3.3.3 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.

3.3.4 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.

3.3.5 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.

3.3.6 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. Way 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.

3.4 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.

3.5 Third Party Access:

Name of Third Party/ Vendor	Type of Access and Connectivity to data
Drata	API-based read-only integration to internal systems (e.g., GitHub, Google Workspace, Cloudflare) for compliance evidence collection. No write or modify access.
Cloudflare	Access to network metadata and edge logs to provide CDN, WAF, and DDoS protection. No direct access to customer data.
Zendesk	Access to customer contact data and support ticket metadata for helpdesk operations.
GitHub	Source control and CI/CD automation with access to internal repositories; uses SSO + MFA for access control.

DC 4: Disclosures About Identified Security Incidents

1. **Incidents Pertaining as of October 01, 2025**
    1. No significant security incidents have occurred prior to or on October 01, 2025 that would have a material effect on the suitability of the design of the controls or description of the system covered in Section 3 of this report.
2. **Incidents Subsequent to October 01, 2025**
    1. Management is not aware of any incidents that occurred subsequent to October 01, 2025 covered by Section 3 of this report through the date of the service auditor's report that would have a significant effect on management's assertion and description of its system.

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements Were Achieved

5.1 Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Hashforest Technology LLC's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Hashforest Technology LLC's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example. Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

5.2 Commitment to Competence

Hashforest Technology LLC's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge. Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

5.3 Management's Philosophy and Operating Style

The Hashforest Technology LLC management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us. The management team meets frequently to be briefed on technology changes that impact the way Hashforest Technology LLC can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Hashforest Technology LLC to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers. Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

5.4 Organizational Structure and Assignment of Authority and Responsibility

Hashforest Technology LLC's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities. Hashforest Technology LLC's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entitys objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

5.5 Human Resource Policies and Practices

Hashforest Technology LLC's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Hashforest Technology LLC's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

5.6 Risk Assessment Process

The risk management responsibilities within Hashforest Technology LLC are clearly defined to ensure comprehensive oversight and accountability. Specific roles are assigned for managing risks, with each asset and risk having an identified owner responsible for its assessment and treatment. The policy mandates that risk owners assess the impact and likelihood of risks materializing, and they are accountable for implementing and overseeing mitigation strategies. Additionally, the results of risk assessments and subsequent reviews must be documented in a Risk Assessment Report, ensuring a structured reporting and escalation procedure. **Risk Management Process** Hashforest Technology LLC employs a systematic risk management process that encompasses the identification, assessment, and treatment of risks. The process begins with identifying all assets within the scope of the information security program, followed by listing threats and vulnerabilities associated with each asset. Each risk is evaluated based on its impact and likelihood, and a risk level is calculated. The company addresses various categories of risks and employs several mitigation strategies, including the development of security controls, risk transfer, risk avoidance, and risk acceptance. Regular reviews and updates to the Risk Assessment Report ensure continuous monitoring and reassessment of risks. **Risk Analysis Method** The method for evaluating risks at Hashforest Technology LLC involves a detailed scoring system that calculates risk levels based on impact and likelihood measures. Impact levels range from incidental to extreme, with specific criteria defining each level's consequences. Likelihood values are assigned based on the probability of occurrence, ranging from rare to almost certain. The risk level is determined by multiplying the impact score by the likelihood score, and risks are categorized as low, medium, high, or critical based on the resulting value. This structured approach informs the prioritization of risks and the corresponding actions to be taken.

5.7 Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Hashforest Technology LLC's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Hashforest Technology LLC addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Hashforest Technology LLC's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

5.8 Information Management and Communication

Hashforest Technology LLC ensures effective communication of risk-related responsibilities and expectations through its Code of Conduct, which mandates that all employees, contractors, consultants, and service providers adhere to established policies and procedures. Leadership plays a crucial role in disseminating standards and reviewing the Code with their teams to ensure familiarity and compliance. Employees are obligated to report any suspected violations or concerns to their supervisors, management, or the Compliance Officer, fostering a proactive approach to risk management. The company's communication channels are aligned with the risk assessment process, emphasizing the importance of integrity, prompt action, and thorough understanding of compliance policies specific to job responsibilities. Hashforest Technology LLC uses several information and communication channels internally to share information with management, employees, contractors, and customers. Hashforest Technology LLC uses chat systems and email as the primary internal and external communications channels. Structured data is communicated internally via SaaS applications and project management tools. Finally, Hashforest Technology LLC uses in-person and video â€œall handsâ€ meetings to communicate company priorities and goals from management to all employees.

5.9 Monitoring Controls

Anomalies and potential security incidents are detected through continuous monitoring of logs and alerting mechanisms, including intrusion detection systems and change-detection mechanisms. The protection and retention of logs are prioritized, with access restricted to authorized personnel and safeguards in place to prevent unauthorized modifications. Logs are backed up to secure, central servers, and subjected to routine reviews to maintain accountability. Failures in critical security controls are promptly addressed in accordance with incident response procedures. The responsibilities for reviewing and responding to logs are clearly defined, ensuring that any security issues are identified and remediated effectively, supporting compliance and forensic analysis.

5.10 Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

DC 6: Complementary User Entity Controls (CUECs)

Hashforest Technology LLC's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Hashforest Technology LLC's services to be solely achieved by Hashforest Technology LLC control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Hashforest Technology LLC's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

- User entities are responsible for understanding and complying with their contractual obligations to Hashforest Technology LLC Inc
- User entities are responsible for notifying Hashforest Technology LLC of changes made to technical or administrative contact information.
- User entities are responsible for maintaining their own system(s) of record.
- User entities are responsible for ensuring the supervision, management, and control of the use of Hashforest Technology LLC services by their personnel.
- User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Hashforest Technology LLC services.
- User entities are responsible for providing Hashforest Technology LLC with a list of approvers for security and system configuration changes for data transmission.
- User entities are responsible for immediately notifying Hashforest Technology LLC of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

DC 7: Complementary Subservice Organization Controls (CSOCs)

Hashforest Technology LLC uses subservice organizations in support of its system. Hashforest Technology LLC's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Hashforest Technology LLC to be achieved solely by Hashforest Technology LLC. Therefore, user entity controls must be evaluated in conjunction with Hashforest Technology LLC's controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

- Hashforest Technology LLC periodically reviews the quality of the outsourced operations by various methods including
- Review of subservice organizations' SOC reports;
- Regular meetings to discuss performance; and,
- Non-disclosure agreements.

Phala Clouds 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 trusted infrastructure providers such as OVH and DCML. The compute infrastructure combines CPU nodes and GPU clusters supporting IntelÂ® Trust Domain Extensions (TDX) and NVIDIA Confidential Compute to ensure hardware-level isolation and data protection during processing. All infrastructure is operated under strict physical and logical access controls, while auxiliary services including global DNS, CDN, and DDoS protection are provided by Cloudflare.

Category	Criteria	Control
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
Security	CC 6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.

Security	CC 6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC 6.4	Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
Security	CC 6.4	Access to server locations is managed by electronic access control devices.
Security	CC 7.2	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 trusted infrastructure providers such as OVH and DCML. The compute infrastructure combines CPU nodes and GPU clusters supporting Intel Trust Domain Extensions (TDX) and NVIDIA Confidential Compute to ensure hardware-level isolation and data protection during processing. All infrastructure is operated under strict physical and logical access controls, while auxiliary services including global DNS, CDN, and DDoS protection are provided by Cloudflare. is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
Security	CC 7.2	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 trusted infrastructure providers such as OVH and DCML. The compute infrastructure combines CPU nodes and GPU clusters supporting Intel Trust Domain Extensions (TDX) and NVIDIA Confidential Compute to ensure hardware-level isolation and data protection during processing. All infrastructure is

		operated under strict physical and logical access controls, while auxiliary services including global DNS, CDN, and DDoS protection are provided by Cloudflare. is responsible for protecting data centers against disruption in power supply by an uninterruptible power supply.
Security	CC 7.2	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 trusted infrastructure providers such as OVH and DCML. The compute infrastructure combines CPU nodes and GPU clusters supporting Intel Trust Domain Extensions (TDX) and NVIDIA Confidential Compute to ensure hardware-level isolation and data protection during processing. All infrastructure is operated under strict physical and logical access controls, while auxiliary services including global DNS, CDN, and DDoS protection are provided by Cloudflare. oversees the regular maintenance of environmental protections at data centers.

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

All Security criteria were applicable to Hashforest Technology LLC's system.

DC 9: Disclosures of Significant Changes in the Last 1 Year

1. **Significant Changes and Events as of October 01, 2025**
    1. No significant changes and events have occurred prior to or on October 01, 2025 that would have a material effect on the suitability of the design of the controls and/or description of the system covered in Section 3 of this report.
2. **Significant Changes and Events subsequent to October 01, 2025**
    1. Management is not aware of any changes that occurred subsequent to **October 01, 2025** covered by Section 3 of this report through the date of the service auditor's report that would have a significant effect on management's assertion and description of its system.

PRESCIENT ASSURANCE

SECTION 4

Testing Matrices

Applicable Trust Services Criteria and Related Control Activities

Trust ID	Trust Services Criteria	Control Description
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Management conducts periodic evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	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.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Personnel, including employees and contractors, are required to sign an agreement that outlines confidentiality requirements (e.g., non-disclosure agreements) prior to hire.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Hashforest Technology LLC maintains a documented code of conduct. Eligible personnel are required to acknowledge Hashforest Technology LLC's code of conduct during onboarding and annually thereafter.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Company policies are accessible to all employees and, as applicable, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	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.
CC1.2	The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors, owners, senior leadership, or equivalent body, meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.
CC1.2	The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	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.).
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	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.).
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees (e.g., through the company's HRMS, intranets, etc.) and is updated upon changes to the organizational structure.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Hashforest Technology LLC 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.).
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Management conducts periodic evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Hashforest Technology LLC maintains a documented code of conduct. Eligible personnel are required to acknowledge Hashforest Technology LLC's code of conduct during onboarding and annually thereafter.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	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.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Management conducts periodic evaluations of performance against established goals and objectives for eligible personnel in accordance with company policies and procedures.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Hashforest Technology LLC maintains a documented code of conduct. Eligible personnel are required to acknowledge Hashforest Technology LLC's code of conduct during onboarding and annually thereafter.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees (e.g., through the company's HRMS, intranets, etc.) and is updated upon changes to the organizational structure.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Company policies are accessible to all employees and, as applicable, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	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.).
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	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.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Hashforest Technology LLC has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Hashforest Technology LLC uses compliance automation software to identify, select, and continuously monitor internal controls.

CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Hashforest Technology LLC 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.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	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.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	An organizational chart is in place to describe the organizational structure and reporting lines. The chart is available to all employees (e.g., through the company's HRMS, intranets, etc.) and is updated upon changes to the organizational structure.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Hashforest Technology LLC maintains a documented code of conduct. Eligible personnel are required to acknowledge Hashforest Technology LLC's code of conduct during onboarding and annually thereafter.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Hashforest Technology LLC 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.).
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company's board of directors, owners, senior leadership, or equivalent body, meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Company policies are accessible to all employees and, as applicable, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	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.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Hashforest Technology LLC uses compliance automation software to identify, select, and continuously monitor internal controls.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	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.).
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's board of directors, owners, senior leadership, or equivalent body, meets at least annually with management to review company performance, strategic objectives, compliance initiatives,

		and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Hashforest Technology LLC maintains a publicly available terms of service for use of the system. All users must agree to the terms of service prior to using the system.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Hashforest Technology LLC communicates system changes via release notes or change log in the company's website or via periodic communications.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Personnel, including employees and contractors, are required to sign an agreement that outlines confidentiality requirements (e.g., non-disclosure agreements) prior to hire.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Hashforest Technology LLC's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Hashforest Technology LLC 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.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Hashforest Technology LLC 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).
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Hashforest Technology LLC's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Hashforest Technology LLC uses compliance automation software to identify, select, and continuously monitor internal controls.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Hashforest Technology LLC 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. Hashforest Technology LLC 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.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Hashforest Technology LLC 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).
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Hashforest Technology LLC 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 Hashforest Technology LLC's requirements. Results of the review and action items, if any, are documented.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Hashforest Technology LLC 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.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Hashforest Technology LLC 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.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Hashforest Technology LLC's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Hashforest Technology LLC 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).
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Hashforest Technology LLC 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.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Hashforest Technology LLC uses compliance automation software to identify, select, and continuously monitor internal controls.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Hashforest Technology LLC 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.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Hashforest Technology LLC uses compliance automation software to identify, select, and continuously monitor internal controls.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Hashforest Technology LLC's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Hashforest Technology LLC 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).
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Hashforest Technology LLC uses compliance automation software to identify, select, and continuously monitor internal controls.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	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.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	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.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Hashforest Technology LLC 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.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and The Board of Directors, as appropriate.	Hashforest Technology LLC 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.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and The Board of Directors, as appropriate.	Hashforest Technology LLC's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and The Board of Directors, as appropriate.	Hashforest Technology LLC 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).
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and The Board of Directors, as appropriate.	Hashforest Technology LLC uses compliance automation software to identify, select, and continuously monitor internal controls.
CC4.2	The entity evaluates and communicates	The company's board of directors, owners, senior leadership, or

	internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and The Board of Directors, as appropriate.	equivalent body, meets at least annually with management to review company performance, strategic objectives, compliance initiatives, and security and privacy risk and mitigation strategies. Meeting minutes, including decisions made and action items, are documented.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Hashforest Technology LLC uses compliance automation software to identify, select, and continuously monitor internal controls.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Hashforest Technology LLC's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	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.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Hashforest Technology LLC 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).
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Hashforest Technology LLC's management has documented a risk treatment plan to formally manage risks identified in risk assessment activities.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Company policies are accessible to all employees and, as applicable, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Hashforest Technology LLC 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).
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Hashforest Technology LLC uses compliance automation software to identify, select, and continuously monitor internal controls.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	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.

CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	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.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Hashforest Technology LLC 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.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Hashforest Technology LLC 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.).
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Hashforest Technology LLC has established and documented a policy that outlines requirements for the management and tracking of company assets.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Hashforest Technology LLC maintains a documented code of conduct. Eligible personnel are required to acknowledge Hashforest Technology LLC's code of conduct during onboarding and annually thereafter.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Hashforest Technology LLC 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.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Hashforest Technology LLC has defined and documented an information security policy and other topic-specific policies as needed to support the functioning of internal control.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Hashforest Technology LLC has a documented policy that establishes requirements for the use of cryptographic controls.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Hashforest Technology LLC has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Company policies are accessible to all employees and, as applicable, third parties such as contractors. Personnel are required to acknowledge the information security policy and other topic-specific policies based on their job duties during onboarding and annually thereafter.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Hashforest Technology LLC has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	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.).

CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Hashforest Technology LLC has a documented acceptable use policy that outlines requirements for personnel's usage of company assets.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Hashforest Technology LLC 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.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	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.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Authentication to systems requires the use of multi-factor authentication.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Administrative or privileged access to systems, resources, and functions is restricted to authorized personnel.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	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.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Authentication to systems requires the use of unique identities.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Data in transit is encrypted using strong cryptographic algorithms.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Network security controls are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Data at rest is encrypted using strong cryptographic algorithms.

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Hashforest Technology LLC has a documented policy that establishes requirements for the use of cryptographic controls.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Hard-disk encryption is enabled on all company-managed devices.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	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).
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.)
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Hashforest Technology LLC 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.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	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.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	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.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	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).
CC6.2	Prior to issuing system credentials and granting system access, the entity registers	Hashforest Technology LLC has developed and documented a policy that outlines requirements for access control.

	and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	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.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	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.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Hashforest Technology LLC has developed and documented a policy that outlines requirements for access control.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	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).
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	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.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Hashforest Technology LLC has a documented policy that outlines requirements for physical security.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's	Hashforest Technology LLC disposes of data on hardware through secure means, such as wiping and hard drive destruction, in accordance with documented policies and procedures.

	objectives.	
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Hashforest Technology LLC has documented policies and procedures for erasure or destruction of information that has been identified for disposal.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Data in transit is encrypted using strong cryptographic algorithms.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Data at rest is encrypted using strong cryptographic algorithms.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network security controls are in place to limit inbound and outbound traffic to the environment to only what is necessary based on business justification. All other traffic is specifically denied.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	A web application firewall is in place to protect public-facing web applications from outside threats.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Remote access to production systems is only available through an encrypted connection (e.g., encrypted virtual private network, SSH, etc.)
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	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.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Hashforest Technology LLC 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.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Authentication to systems requires the use of multi-factor authentication.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Hashforest Technology LLC has a documented a policy that outlines the procedures and technical measures to be implemented at the organization to protect the confidentiality, integrity, and availability of data.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Hard-disk encryption is enabled on all company-managed devices.
CC6.7	The entity restricts the transmission, movement, and removal of information to	Automated operating system (OS) updates are enabled on company-managed devices to install security patches.

	authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Data in transit is encrypted using strong cryptographic algorithms.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Hashforest Technology LLC has implemented automated mechanisms (e.g., unattended upgrades, automated patching tools, etc.) to install security fixes to systems.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Anti-malware software is installed on all company-managed devices.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Hashforest Technology LLC 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.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	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.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	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.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Anti-malware software is installed on all company-managed devices.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Automated operating system (OS) updates are enabled on company-managed devices to install security patches.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to	Hashforest Technology LLC conducts vulnerability scans of the production environment as dictated by company policy and

	identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	compliance requirements. Results are reviewed by company personnel and vulnerabilities are tracked to resolution in accordance with company policies.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	A web application firewall is in place to protect public-facing web applications from outside threats.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Hashforest Technology LLC 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.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	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.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Hashforest Technology LLC documents a post-mortem review for identified incidents that includes incident metadata, root-cause analysis, documentation of evidence, summary of containment, eradication, and recovery actions, timelines, incident metrics, evidence of internal and external communications, estimation of impact and scope, and lessons learned, as applicable, in accordance with company policies and procedures.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Hashforest Technology LLC has a documented 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.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Hashforest Technology LLC 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.).
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Hashforest Technology LLC 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.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives	Hashforest Technology LLC 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,

	(security incidents) and, if so, takes actions to prevent or address such failures.	simulations, etc.). The documented plan and procedures are updated if necessary based on the results of the test.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Hashforest Technology LLC 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.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Hashforest Technology LLC 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.).
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Hashforest Technology LLC has a documented 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.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Hashforest Technology LLC 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.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Hashforest Technology LLC documents a post-mortem review for identified incidents that includes incident metadata, root-cause analysis, documentation of evidence, summary of containment, eradication, and recovery actions, timelines, incident metrics, evidence of internal and external communications, estimation of impact and scope, and lessons learned, as applicable, in accordance with company policies and procedures.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Hashforest Technology LLC has a documented 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.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Hashforest Technology LLC 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.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Hashforest Technology LLC documents a post-mortem review for identified incidents that includes incident metadata, root-cause analysis, documentation of evidence, summary of containment, eradication, and recovery actions, timelines, incident metrics, evidence of internal and external communications, estimation of impact and scope, and lessons learned, as applicable, in accordance with company policies and procedures.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security	Hashforest Technology LLC has identified and documented roles and responsibilities for incident management (e.g., roles and

	incidents.	responsibilities for invoking the incident management process, incident leads, incident handlers, communication coordinators, technical advisors, legal advisors, etc.).
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Hashforest Technology LLC 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.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Pre-production environments (e.g., development, testing, etc.) are separated from production environments and the separation is enforced with access controls.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Changes are peer-reviewed and approved prior to deployment by an individual different from the developer to maintain segregation of duties. Review requirements are enforced through automated mechanisms such as branch protection settings in the production code repository.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Hashforest Technology LLC uses a version control system to manage source code, change documentation and tracking, release labeling, and other change management tasks. Access to the version control system is restricted to authorized personnel.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Hashforest Technology LLC has developed policies and procedures governing the system development life cycle, including requirements, design, implementation, testing, and deployment.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Hashforest Technology LLC has implemented automated mechanisms (e.g., unattended upgrades, automated patching tools, etc.) to install security fixes to systems.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Hashforest Technology LLC has a defined business continuity plan that outlines strategies for maintaining operations during a disruption.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Hashforest Technology LLC has a documented disaster recovery plan that outlines roles, responsibilities and detailed procedures for recovery of systems in the event of a disaster scenario.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Hashforest Technology LLC has a documented 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.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Hashforest Technology LLC has a documented policy that outlines requirements for managing vendor and third-party relationships through their entire life cycle.
CC9.2	The entity assesses and manages risks	Hashforest Technology LLC maintains a vendor/third party register

	associated with vendors and business partners.	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. Hashforest Technology LLC 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.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Hashforest Technology LLC 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 Hashforest Technology LLC's requirements. Results of the review and action items, if any, are documented.

Signed and Accepted by

Prescient Assurance

Prescient Assurance LLC

Lin Tong

Lin Tong

CEO of Hashforest Technology

Hashforest Technology LLC

Certificate of Completion

Document ID: 2c8a63a6-367d-456b-a6b4-9d4ee4f1759d

Document Title: Report

Status: Completed

Name of the Company: Hashforest Technology LLC

Audit Trail

Username	Email	Action	IP Address	Date/Time
Markel Samuel	Markel.samuel@prescientassurance.com	Report Shared with doyle@phala.network	10.0.7.168	2025-12-15 20:27:26
Markel Samuel	Markel.samuel@prescientassurance.com	Report Shared with marvin@phala.network	10.0.7.168	2025-12-15 20:39:56
Akhil Das	akhil.das@prescientsecurity.com	report Signed by Admin	117.216.72.176	2025-12-18 18:50:54
Julia Breker	julia.breker@prescientsecurity.com	Report Shared with marvin@phala.network	10.0.15.140	2025-12-18 21:38:47
Lin Tong	marvin@phala.network	report Signed by Client	107.131.79.101	2025-12-19 00:38:30

Management Representation Letter

From: Hashforest Technology LLC

To:

Prescient Assurance LLC

1900 Church Street, Suite 300,

Nashville, TN 37203

+1 646 209 7319

info@prescientassurance.com

In connection with your engagement to report on Hashforest Technology LLC's (service organization) description of its Phala Cloud system titled Phala Cloud System Description as of October 01, 2025 (description) based on the criteria set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)(2018 description criteria) and the suitability of the design of the controls included in the description as of October 01, 2025 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the trust services criteria relevant to "Security" set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022) (2017 applicable trust services criteria), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion about whether the description presents the system that was designed and implemented as of October 01, 2025 in accordance with the description criteria and whether the controls stated in the description were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, if the controls operated effectively as of October 01, 2025.

We confirm, to the best of our knowledge and belief, as of December 19, 2025, the date of your report, the following representations made to you during your examination

1. We are responsible for the preparation and presentation of the description, including the completeness, accuracy, and method of presentation of the description, in accordance with the description criteria and the suitability of the design of the controls included in the description to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
2. We also are responsible for our written assertion that accompanies the description of the system, both of which will be provided to you and users of the report. We are responsible for the completeness, accuracy, and method of presentation of the assertion and for having a reasonable basis for it. We reaffirm our assertion attached to the description.
3. We have evaluated the presentation of the description in accordance with the description criteria and the suitability of the design of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and all relevant matters have been considered and reflected in our evaluation and

in our assertion.

4. We have disclosed to you all known matters that may contradict the presentation of the description or the suitability of the design of the controls stated in the description, or our assertion.
5. 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 included in the description.
6. 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.
7. We are responsible for selecting the trust services category(ies) and criteria to be included within the scope of our examination and determining that such criteria are suitable, will be available to the intended users and they are appropriate for our purposes. We are responsible for stating the applicable trust services criteria and related controls in the description. For any additional criteria specified by law, regulation, or another party, we are responsible for identifying that party in the description.
8. We are responsible for determining the effect on our service commitments and system requirements of any services provided to the service organization by other organizations and determining whether those entities are subservice organizations. We are also responsible for determining whether we will use the carve-out method or inclusive method to present information about services provided at any subservice organizations in our description.
9. We are responsible for identifying and analyzing the risks that threaten the achievement of our service commitments and system requirements based on the applicable trust services criteria.
10. We are responsible for designing, implementing, and documenting controls that are suitably designed to provide reasonable assurance that our service commitments and system requirements are achieved based on the applicable trust services criteria.
11. We are responsible for specifying the principal service commitments made to user entities and the system requirements necessary to operate the system and meet commitments to our business partners.
12. We have provided you with the following:
    1. 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.
    2. Access to additional information you have requested from us for the purpose of the engagement.
    3. Unrestricted access to persons within the appropriate parties from whom you determined was necessary to obtain evidence relevant to your engagement.
13. We believe the effects of uncorrected misstatements (such as discrepancies in the description or deficiencies in the controls described), if any, are immaterial, individually and in the aggregate, to the presentation of the description in accordance with the description criteria or to the suitability of the design of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
14. We have disclosed to you any known events subsequent to the period covered by the description of the system up to the date of this letter that would have a material effect on the presentation of the description or the suitability of the design of the controls, or our assertion.
15. 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.
16. 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.
17. We also have disclosed to you all instances about which we are aware of the following:
    1. Misstatements and omissions in the description.
    2. Instances in which controls have not been suitably designed or implemented as described.
18. We have disclosed to you all identified system incidents that resulted in a significant impairment of the service organization's achievement of its service commitments and system requirements as of October 01, 2025.

19. 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.
20. We have responded fully to all inquiries made to us by you during the examination.
21. We understand that your report is intended solely for the use and information of management of the service 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.

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and was designed for the purpose of expressing an opinion about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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.

Lin Tong

CEO of Hashforest Technology

Hashforest Technology LLC