System and Organization Control Report Relevant to Security, Availability and Confidentiality + HIPAA Mapping

(SOC 3)

April 01, 2025 – July 31, 2025

Deloitte.

Brightman Almagor Zohar & Co.
1 Azrieli Center, 6701101 P.O.B
16593, Tel Aviv, Israel
Tel: +972 (3) 608 5555
www2.deloitte.com/il/en.html

Independent Service Auditors' Report

Nebius BV

Schiphol Boulevard 165,
1118 BG Schiphol, the Netherland

Scope

We have examined management of Nebius BV's (the "Service Organization" or "Nebius") accompanying assertion titled "Management of Nebius BV's Assertion" ("management's assertion") that the controls within Nebius's full-stack infrastructure for AI system ("system") were effective throughout the period April 01, 2025 to July 31, 2025 to provide reasonable assurance that Nebius's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality ("applicable trust services criteria") set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria and the security requirements set forth in the HIPAA Administrative Simplification (Code of Federal Regulations, Title 45, Sections 164.306-316) ("HIPAA Security") ("applicable criteria").

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nebius, to achieve Nebius's service commitments and system requirements based on the applicable trust services criteria. The Description presents Nebius's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Nebius's controls. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Nebius BV uses third-party providers for data center and colocation services ("subservice organizations") ("subservice organizations"). The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nebius BV, to achieve Nebius BV's service commitments and system requirements based on the applicable trust services criteria. The Description presents Nebius BV's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Nebius BV's controls. The Description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Management of Nebius BV is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Nebius BV service commitments and system requirements would be achieved. Management of Nebius has provided the accompanying assertion titled, "Management of Nebius BV's Assertion" (the "Assertion") about the Description and the suitability of the design and operating effectiveness of controls stated therein. Management of Nebius 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.

Deloitte.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of design and operating effectiveness of controls stated in the Description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the 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 and operating effectively to provide reasonable assurance that Nebius's service commitments and system requirements would be 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 a Description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria.

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

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA. We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness 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.

Deloitte.

Opinion

In our opinion, management's assertion that the controls over the information systems and technology supporting Nebius full-stack infrastructure for AI system were effective throughout the period April 01, 2025 to July 31, 2025 , to provide reasonable assurance that Nebius BV's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Brightman Almagor Zohar & Co.
Certified accountants
A firm in the Deloitte Global Network

October 19, 2025

Deloitte.

Management of Nebius BV's Assertion

We are responsible for designing, implementing, operating and maintaining effective controls over the information systems and technology supporting Nebius BV's (the "Service Organization" or "Nebius") Nebius full-stack infrastructure for AI system throughout the period April 01, 2024 to July 31, 2025 to provide reasonable assurance that Nebius BV's service commitments and system requirements relevant to security, confidentiality and availability were achieved based on the trust services criteria (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity ,Confidentiality, and Privacy, in AICPA Trust Services Criteria Our description of the boundaries of the system is presented in Attachment A below and identifies the aspects of the system covered by our assertion. Our description of the boundaries of the system is presented in Attachment A below and identifies the aspects of the system covered by our assertion.

Nebius BV uses third-party providers for data center and colocation services. These providers are responsible for the physical hosting, maintenance, and security of the environments that support Nebius's operations ("subservice organizations"). The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nebius BV, to achieve Nebius BV's service commitments and system requirements based on the applicable trust services criteria. The Description presents Nebius BV's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Nebius BV's controls. The Description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 01, 2025 to July 31, 2025 , to provide reasonable assurance that Nebius BV's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality and availability (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security ("applicable trust services criteria"). Nebius's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nebius, to achieve Nebius's service commitments and system requirements based on the applicable trust services criteria. The Description presents Nebius's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Nebius's controls. The Description does not extend to controls of the user entities.

We assert that the controls within the system were effective throughout the period April 01, 2025 to July 31, 2025 to provide reasonable assurance that Nebius BV's service commitments and system requirements were achieved based on the applicable trust services criteria.

Deloitte.

Attachment A

Nebius BV's Description of the Boundaries of its System

Nebius BV Company Overview

Nebius BV is a technology company building full-stack infrastructure for AI, including large-scale GPU clusters, an AI-native cloud platform, and tools and services for developers. Headquartered in Amsterdam and listed on Nasdaq (ticker:NBIS), the Company has a global footprint with R&D hubs across Europe, North America and Israel.

Nebius AI Cloud is an AI cloud platform built for intensive AI workloads. The Nebius cloud platform delivers a cost-effective, robust, and customizable full-fledged cloud computing platform with over 50 services and solutions. Nebius offers companies scalable infrastructure, multi-cloud solutions, data storage services, AI computing and services, and more.

Overview of Nebius BV services

Nebius provides a comprehensive AI infrastructure ecosystem that covers all needs for AI and ML practitioners, from data preparation and model training to inference deployment and scaling, enabling organizations to build complete AI solutions.

AI Cloud

Full-stack AI infrastructure platform that provides scalable GPU clusters, high-performance storage, and managed services for AI model training and deployment. The platform integrates NVIDIA GPU accelerators (H100, H200, B200, B300, GB200) with InfiniBand networking and Kubernetes/Slurm orchestration to support intensive AI workloads from individual experiments to large-scale enterprise deployments. Nebius also provides their own managed Slurm-based scheduler (Soperator) for large-scale AI training workloads.

AI Studio

Inference-as-a-Service platform provides hosted AI model inference capabilities through API endpoints, eliminating the need for customers to maintain their own inference infrastructure. The service enables organizations to access pre-trained open-source AI models for real-time and batch inference, model fine-tuning, and customization without requiring MLOps expertise or infrastructure management.

TractoAI

Data-centric serverless platform for AI workloads provides end-to-end data processing, model training, and distributed computing capabilities. The platform enables seamless data preparation, exploration, and large-scale distributed training across multiple data types and formats.

Subservice organizations

Third-party management in data centers plays a critical role in ensuring operational efficiency, security, and compliance, enabling organizations to focus on their core business objectives. As data centers grow in complexity and resource requirements, the company leverages specialized third-party providers for key functions such as infrastructure maintenance, monitoring, security, and compliance management. By relying on external expertise, the company can reduce costs, mitigate

risks, and scale operations effectively. This approach enhances performance, reliability, and supports strategic growth within an increasingly data-driven environment. The company utilizes a range of industry-leading third-party data center providers, each offering robust, secure, and energy-efficient services tailored to enterprise and public sector needs.

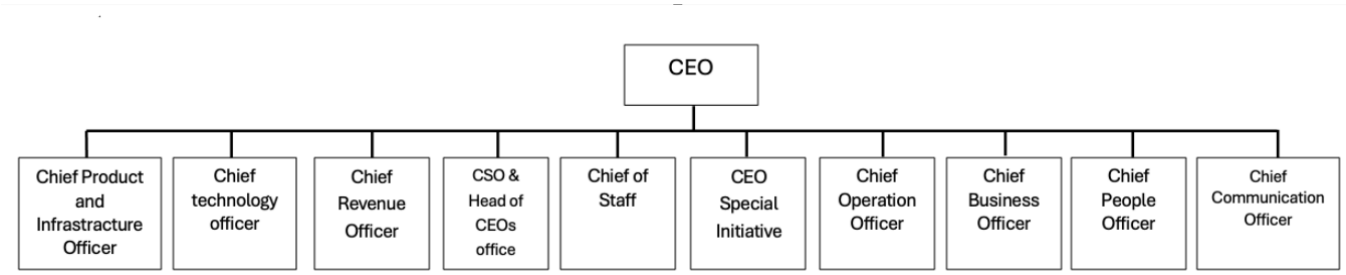
Organizational Structure

Nebius' organizational structure provides the overall framework for planning, directing and controlling operations. It utilizes an approach whereby personnel and business functions are segregated into departments according to job responsibilities, lines of reporting and communications, and allows employees to focus on the specific business issues impacting their customers and to appropriately meet the security requirements. Below is a description of key Nebius management roles:

- **CEO:** The Chief Executive Officer is responsible for providing strategic, financial, and operational leadership for the company and works closely with Nebius BV managing directors, as well as the board of directors and senior leadership team. The CEO responsible for Planning, developing, implementing, and directing the organization's operational and fiscal function and performance.
- **COO:** Nebius BV Chief Operating Officer oversees the company's operations. The COO oversees the day-to-day administrative and operational functions of Nebius BV. The COO Act as co-managing director.
- **CSO:** Chief security officer is responsible for the overall security strategy, encompassing both physical and information security and reporting directly to the company’s CEO.
- **GC:** General Council - The General Counsel (GC) is the chief legal officer responsible for overseeing all legal matters within Nebius BV. The GC is responsible for providing legal advice and guidance to the company's executives and management team, ensuring compliance with laws and regulations, and managing legal risks across all regions Nebius is operating in.
- **Chief product and infrastructure officer** - The Chief Product and Infrastructure Officer is a senior executive responsible for overseeing the development, implementation, and management of the company's technology infrastructure. This role is crucial for ensuring that the cloud services provided are reliable, scalable, and secure.
- **CRO:** Chief Revenue Officer - responsible for overseeing and driving the overall business strategy, operations, and growth of an organization. focuses on aligning business goals with financial objectives, identifying new market opportunities, and enhancing operational efficiency.
- **CTO:** The chief technology officer is responsible for the R&D departments and the software development of the different services on top of the cloud infrastructure.
- CIO - The Chief information Officer makes executive decisions regarding the technological interests of a company. Responsible for outlining the company's technological vision.
- **CISO:** Nebius BV Chief Information Security Officer responsible for establishing and maintaining an organization's information security strategy and framework, overseeing the protection of digital assets, managing cybersecurity tools, and ensure monitoring and proper incident response.
- **CPO:** Chief People Officer: overseeing all aspects of an organization's human resources strategy, including talent acquisition, employee development, culture, and retention. The CPO ensures that the company's workforce is aligned with its overall business goals, fosters a positive work environment, and drives initiatives to enhance employee satisfaction and performance.
- **CFO:** Chief financial officer’s duties include tracking cash flow and financial planning as well as analyzing the company's financial strengths and weaknesses and proposing corrective actions. group
- **CCO -** Chief Communication Officer: responsible for managing and overseeing an organization's internal and external communication strategies. This includes media relations, public relations, corporate messaging, brand management, and crisis communication

Deloitte.

See below a high-level Nebius Organizational Chart:



Roles and Responsibilities

Nebius has formally established requirements that describe the key roles including responsibilities and related job descriptions as required by Nebius officers. With respect to relevant trust principle areas, there is an assignment of responsibility and authority for decision-making in Nebius. Lines of authority and responsibility are clearly established throughout the organization and are communicated through Nebius's management, operating activities, organizational structure, employee job descriptions, organizational policies and procedures. Nebius's employees are required to sign an NDA as part of their employment contract with Nebius while clients sign an NDA within the business contract.

Deloitte.

Attachment B

Principal Service Commitments and System Requirements

Principle Service Commitments and System Requirements

Nebius's security commitments in regards to the systems and operations are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided to user entities. Those objectives are based on the service commitments that Nebius makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that Nebius has established for the services.

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

- Security principles within the fundamental designs of Nebius' system that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit
- Identify and response to cyber threats by proactively monitoring and protecting Nebius' information systems and our customer's data
- Use strong identity management processes to secure data and systems from intrusion.
- Manage infiltration, intrusions, insider threats and anomalies by understanding who is on our networks, why they are on our networks, and what data they have permission to access.

Nebius establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Nebius system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of relevant service provided to its customers.

CC1.0 Control Environment

The control environment of the company plays a fundamental role in fostering a culture of security and compliance within the organization. It sets the tone for all employees, guiding their understanding and the importance of maintaining stringent internal controls. The leadership team, including management and the Board of Directors, actively communicates and reinforces the significance of security protocols, ensuring that all employees are aware of their roles in safeguarding company assets and sensitive information.

This control environment is bolstered by the company's physical security measures, which encompass clear policies and procedures for protecting sensitive data and systems. The company has implemented a comprehensive set of physical security standards, including restricted access to facilities, surveillance systems, and visitor management protocols. These measures help to minimize physical security risks and prevent unauthorized access to company premises, particularly areas housing sensitive and highly sensitive information.

By establishing strong security foundations and clearly defined roles for employees and the physical security team, the company ensures that it can effectively achieve its strategic objectives while

meeting compliance requirements. This environment supports operational efficiency, risk mitigation, and the protection of valuable assets, all while adhering to legal and regulatory obligations.

Board of directors - The Board of Directors of Nebius plays a critical role in the governance and oversight of the organization's operations, including the effectiveness of its system of internal controls relevant to security, availability, confidentiality, and privacy. The Board ensures that the company's strategic direction aligns with its risk management framework, compliance obligations, and Nebius' business strategy.

The Board is composed of a diverse group of individuals with expertise in cloud technology, cybersecurity, compliance, finance, and corporate governance. A majority of the Board members are independent, ensuring objective oversight and decision-making. in addition, the board receives regular reports from executive leadership, including the Chief Security Officer (CSO), Chief Infrastructure Officer (CIO), and Chief Technology Officer (CTO). These reports include:

- Updates on control performance and audit results
- Security incident reports and response actions
- Risk assessments and mitigation strategies
- Compliance status with SOC 2 and other regulatory frameworks

Management Philosophy and Operating Style

Nebius is committed to maintaining a robust security posture through a clearly defined security structure, clear R&R and defined frameworks and standards to ensure the safety of its products and services and increase customer trust.

Nebius management adopted several standards and frameworks, security and privacy. Management commitment includes the following:

- Allocate appropriate resources to support security and privacy initiatives
- Appoint a quarterly Security Steering Committee to discuss strategic security decisions
- Appointed officials who will lead the company's security and privacy domains and issue letters of appointments accordingly
- Review the organization's security posture and status annually to assess effectiveness and identify areas for improvement
- Nebius management is committed to participate in drills and tabletop exercises as required
- Be notified of major security incidents and disruptive events and ensure appropriate response measures are taken
- Commitment to continual improvement of the Information Security Management System (ISMS)
- Ensure compliance with applicable security requirements

Human Resources Policy and Practices

The competence and integrity of the company's personnel are essential to controlling the environment. The company's human resources policies cover the full employee lifecycle, including recruitment and hiring, onboarding, training, promotions, transfers, and termination. Employees and contractors are subject to thorough background checks, and all new hires are required to undergo mandatory security and privacy training. Access to systems is granted based on the "need-to-know" principle, with role-based access controls in place throughout employment.

The Employee security Life Cycle Policy outlines the different stages each employee undertakes from the pre-employment phase to employee termination. Each phase has different security controls and records of all those activities are kept accordingly.

These policies are reviewed annually by management to ensure they remain aligned with security and compliance standards. The HR team, in collaboration with security teams, actively monitors compliance throughout the employee lifecycle. Any misconduct, especially security violations, is addressed through formal disciplinary actions, with outcomes documented and reviewed by HR, legal, and security teams to maintain accountability and protect sensitive information.

Commitment to Competence

Nebius demonstrates a strong commitment to competence by ensuring that all personnel possess the necessary knowledge, skills, and abilities to perform their roles effectively. This commitment is foundational to the company's ability to design, implement, and operate controls that support the security, availability, confidentiality, and privacy of its cloud services.

Nebius established a formal competency framework that includes:

- **Defined Role Descriptions**: Each role within the organization has a clearly defined set of responsibilities, required qualifications, and expected competencies.
- **Skills Matrix**: A skills matrix is maintained to map employee capabilities against role requirements, ensuring alignment with organizational needs.
- **Job-Specific Training**: Employees receive training tailored to their roles, including secure software development, cloud infrastructure management, incident response, and regulatory compliance.
- **Regular Performance Reviews**: Employee performance is evaluated semi-annually, with a focus on technical competence, adherence to security practices, and contribution to control effectiveness.
- **Board Oversight**: The Board of Directors receives periodic updates on workforce capability, training completion rates, and key talent metrics.

Nebius maintains a robust and proactive approach to ensuring personnel competence. This commitment supports the effective operation of controls and reinforces the organization's ability to meet its service commitments and system requirements.

CC2.0 Information and Communication

Information and communication are integral components of Nebius' internal control system. They involve the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage and control the organization's operations. At Nebius, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Internal communication

Nebius maintains a structured and secure internal communication framework to ensure that all personnel are informed of their responsibilities related to security, privacy, compliance, and operational. Effective internal communication supports the implementation and operation of controls aligned with SOC 2, GDPR, ISO/IEC 27001, and other regulatory and industry standards.

The company maintains an internal informational knowledge base describing the company's environment, user responsibilities and processes for the different divisions.

All internal policies, including security and privacy policy, are published on the company's internal knowledge base and being reviewed annually.

Employees are notified of policy via the HR system and internal collaboration platforms (e.g., Slack). mandatory training content is reviewed in the Learning Management System (LMS) or via a dedicated security platform (e.g., KnowB4).

External communication

Effective external communication is critical to maintaining transparency, trust, and compliance with regulatory and contractual obligations. As a cloud service provider, we recognize the importance of structured, secure, and policy-driven communication with customers, regulators, investors, auditors, and other external stakeholders. Nebius implemented several controls and practices to ensure that external communications are accurate, authorized, and aligned with our security, privacy, and compliance commitments.

The organization defined communication policy for all outbound communications that contain sensitive, confidential, or regulated information. This policy enforced through training, automated controls, and periodic audits.

Nebius has several authorized communication channels including:

- **Corporate email systems** with enforced encryption
- **Customer portals** (Trust center) for sharing customer-facing documents
- **Public relations and media platforms** managed by the communications team
- **Dedicated security email** address to report security issues (Security@nebius.com)

All channels are subject to logging and monitoring to detect unauthorized disclosures or anomalies.

CC3.0 Risk Assessment

Nebius is committed to identifying, assessing, and mitigating risks that could affect its ability to achieve business objectives. Effective risk management is integrated into the company's strategic planning, operational activities, and decision-making processes, ensuring consistent and proactive management of risks across all levels of the organization.

- **Risk Identification and Assessment:**
  The company employs a systematic approach to risk identification and assessment, in alignment with recognized standards such as ISO/IEC 27001. The process includes identifying critical assets—such as information, business processes, and infrastructure—and evaluating the threats and vulnerabilities that may compromise these assets. Risk assessments are conducted regularly, at least annually, and whenever there are significant organizational or environmental changes. The process also includes an evaluation of risks from external sources, such as third-party vendors and supply chain partners.
- **Risk Assessment Framework:**
  Nebius utilizes a consistent methodology for evaluating risks based on the likelihood of their occurrence and their potential impact on the company's confidentiality, integrity, and availability of data and assets. This methodology ensures that each risk is categorized, prioritized, and aligned with the company's risk appetite. The risk assessment process includes identifying the threat source, assessing vulnerabilities, determining risk levels, and assigning responsibility for risk treatment.
- **Risk Treatment and Mitigation:**
  After identifying and assessing risks, the company determines the appropriate risk treatment strategies. These strategies may include risk acceptance, avoidance, mitigation,

or transfer. Mitigation efforts are implemented to reduce either the likelihood or impact of identified risks. Nebius conducts a cost-benefit analysis to ensure that mitigation actions are proportionate to the level of risk. Mitigation efforts are documented, and the effectiveness of these measures is periodically reviewed to ensure alignment with the company's overall security posture and objectives.

- **Ongoing Monitoring and Review:**
  Risk management at Nebius is an ongoing process that includes continuous monitoring of identified risks and periodic reassessments. The company uses tools such as the Scytale GRC system to track and document risks, monitor remediation efforts, and update risk profiles. Regular risk reviews are conducted by senior management, ensuring that risk-related decisions are informed and aligned with business objectives. Risk re-evaluation occurs following significant changes in the company's environment, such as major infrastructure upgrades, mergers, or new regulatory requirements.
- **Risk Appetite and Classification:**
  Nebius defines its risk appetite by evaluating risks based on their potential impact and likelihood of occurrence. Risks are classified into various levels—low, medium, high, or critical—based on their severity. High- and medium-priority risks are prioritized for mitigation, while lower-priority risks are monitored and reviewed periodically to reassess their relevance.

CC4.0 Monitoring Activities

Nebius AI implements monitoring and logging controls to track and audit access to confidential data across its AI cloud. These controls are designed to detect unauthorized access, support forensic investigations, and ensure compliance.

Access Logging
All access to systems and services that handle confidential or sensitive data is logged in real time. Logs capture key metadata including but not limited to the following:

- User identity and role
- Timestamp of access
- Access method
- Resources accessed
- Action performed

Monitoring & Alerting
Logs are continuously monitored using automated security information and event management (SIEM) systems. These systems generate alerts for anomalous or unauthorized access patterns.

Retention & Protection
Access logs are retained in accordance with internal policies and regulatory requirements. Logs are stored securely, protected from tampering, and accessible only to authorized personnel.

Review & Investigation
Security and compliance teams conduct regular reviews of access logs and investigate any suspicious activity. Findings are documented, and corrective actions are taken as needed. Logs also support internal audits and external compliance assessments.

CC6.0 Logical and Physical Access

A Physical and environmental security policy is documented and is reviewed and approved on an annual basis. Nebius has established an organization-wide information security policy designed to protect information at a level commensurate with its regulations, standards and best practices. The

policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission.

Access Control, Users and Permissions Management

Nebius holds sensitive information regarding its customers, employees, and business operations. To safeguard the confidentiality, integrity, and availability of this information, and to prevent unauthorized disclosure that could harm the organization, strict administrative control must be exercised over information access through a defined authorization mechanism.

A critical aspect of information security is user lifecycle management, encompassing the entire process from access requests, account creation, and privilege assignments to modifications and eventual deactivation.

Nebius employees and contractors will not be granted access to any information asset that is not directly needed for their work in Nebius. The Company manages access governance through a roles-based access control matrix based on the job description and responsibilities and implements the following controls to ensure that access management is properly done:

● The Company has established a formal standard for passwords to govern the management and use of authentication mechanisms.

● Nebius requires two-factor authentication over an approved cryptographic channel for authentication to the internal Nebius network from remote locations.

● Nebius has an established key management process in place to support the organization’s use of cryptographic techniques.

● Nebius secures and controls its employees' devices to enforce security settings including - hard-disk encryption, auto patching, password requirement, auto screen-lock, remote wipe capabilities, and deployment of additional policies.

● External access to data stored in S3 is logged and the logs are retained including relevant access request information, such as the data accessor IP address, object, and operation.

To determine the rules and instructions regarding the granting of authorizations to users of the network and information systems, including:

- Establish control mechanisms for authorizations.
- Define roles regarding opening users, granting authorizations to the information systems and ways of handling cases of password unlock.
- Determine the characteristics of passwords to the network and the various information systems.
- Define methods of response in situations of password replacement, loss, and exposure.
- Determine the guidelines and instructions regarding the granting of privileges to users of the company's network and information systems.

Revocation Process

The revocation process is a vital part of access and identity management, ensuring that permissions and credentials are promptly removed when they are no longer needed or become compromised. This process typically involves the systematic deactivation or removal of user accounts, API keys, digital certificates, tokens, or other authentication mechanisms. A well-defined

revocation process includes automated triggers for events such as employee termination, role changes, or credential expiration, as well as manual override capabilities for urgent security situations. Regular audits and access reviews help ensure the effectiveness of revocation measures and reduce the risk of unauthorized access.

Terminated employees complete a termination clearance process on their last day at Nebius while the termination notification is documented and accessible within the Nebius Internal IT management ticket system. This process includes revocation of access permissions to the systems and premises, as well as the return of the property, data and equipment.

Production Environment Logical Access

The production environment is logically separated into distinct "Tenants", each serving as the top-level resource boundary allocated to customers for managing their own cloud resources. Access to each customer's environment through the web interface is conducted using production accounts managed by the company's Identity and Authentication (IAM) service, ensuring only relevant users are authorized.

Access to the production environment is protected and restricted. Privileged access to the company's infrastructure, servers, and production resources is conducted through a VPN connection to the data centers, with each connection uniquely identified at the data center level. This access is limited to authenticated and authorized personnel according to their business function via our Single Sign On system.

Access to production servers and other resources is performed via a secure Identity Aware Proxy and is limited by using our Single Sign On system. Access rights follow the principle of least privilege, with employees granted only the minimum access necessary to perform their duties.

New user access to corporate, production, or development systems is initiated upon notification from the HR department. A ticket is created in the IT management system using a standardized new hire template, which includes all required permissions for the user. Access requests are then approved in the access management system by the appropriate owner or manager.

User access and permissions to systems supporting the production infrastructure are reviewed and approved on a periodic basis. The company prevents customers from accessing physical hosts or instances not assigned to them by enforcing logical separation through virtualization software.

All production media are securely decommissioned in accordance with industry standard practices.

When an employee or contractor no longer requires access, their privileges are promptly revoked. Access revocation follows the procedures outlined in the Access Control Policy and Employee Security Life Cycle Policy, ensuring appropriate removal of rights based on current role and necessity.

Remote Access

When using computing and communication facilities outside of the secure office environment, special care should be taken to ensure that information is not compromised. Protection must be in place to avoid unauthorized access to or disclosure of information, including ensuring your screen cannot be seen by others and that equipment is not left unattended.

Access to Nebius' network from overseas is subject to additional controls to ensure compliance with relevant legislation, which may result in additional personal liability for users.

Deloitte.

Physical Access

- Access to the Nevius company site will be secured through an access control system.
- Company employees will be equipped with personal badges, each configured with access permissions according to the employee's role.
- Badge permissions will be granted to each employee under the responsibility and control of the company's Physical Security Department.
- Upon termination of an employee's employment, personal access permissions will be revoked, and the badge will be deactivated.
- Entry will be made with approval and under the supervision of an authorized party after identification.

Visitors

Visitors to Nebius premises are required to be always accompanied by a Nebius employee during their stay.

Employees encountering unfamiliar or suspicious people in the office space need to immediately report to the site's physical security manager / facility manager / office manager or the HQ physical security team.

Visitors are not allowed to access or connect to Nebius' network or equipment. It is forbidden for any employee to grant a visitor access to the office without escorting the individual to the employee that they arrived to visit.

All Nebius visitors are required to sign in/out at the front desk. Sign-in/out will be accomplished using a Visitor Management System.

Visitors' logs are documented; logs are reviewed in case of security incidents.

All visitors will enter the company's offices through the reception desk.

A company employee will accompany the visitor, lead them to the designated place, and make sure that the visitor carries an identification tag for the duration of his visit. The visitor must be accompanied throughout his visit, including at the reception desk at the end of the visit. The obligation to accompany visitors applies to all company employees.

The security manager will brief the company's employees on this subject upon their recruitment and as part of refresher training.

Visitors must not enter work areas that contain classified information, if necessary, employees must make sure that the work environment does not contain identifiable information.

Recurring visitors will be allowed to enter unaccompanied.

Environmental and physical Controls in the Data Centers

There are several types of data centers type that Nebius maintain, including:

- Fully owned site by Nebius, including on-site Nebius' employees (Such as Finland DC) Co-location site – hosted within an existing data center and maintained by another company, which provides full infrastructure and environmental services and controls. Nebius is responsible only for the specific room where its servers are located.

- Built-to-suit – a site owned and managed by another company but built according to Nebius' specific physical security and environmental requirements.
- Nebius system components are replicated across multiple data centers to handle environmental events such as access control, surveillance cameras, field audits, incident investigations, and collaboration with local security trustees at each site. in addition to that that, each Data center has:
- Fire Detection and Suppression – Automatic fire detection and suppression equipment have been installed to reduce risk.
- Climate and Temperature Controls – maintain a constant operating temperature and humidity level for all hardware.
- Network Redundancy – internet connectivity has redundant lines at every data center as well as dual-line cross data center connectivity.
- Redundant Power – the data center electrical power systems are designed to be fully redundant and maintainable without impact on operations, 24 hours a day, and Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure. Data centers use generators to provide backup power for the entire facility.

CC7.0 System Operations

Security and Architecture

Nebius provides a secure, reliable, and resilient AI cloud platform built for intensive AI workloads designed based on industry's best practices. The Nebius cloud platform offers companies scalable infrastructure, multi-cloud solutions, database management system security, application controls, and intrusion detection monitoring solutions. Nebius utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. A ticketing system is used for logging incidents, assigning severity ratings, and tracking their resolution for effective monitoring. Additionally, security incidents detected are communicated and reviewed by the security teams so ensure effective response in a timely manner.

Data Center Security

Sensitive information and personal data concerning the company and its customers is designed and managed according to security best practices as well as a variety of security compliance standards and regulations.

The environmental protection managed within the Data centers includes, but not limited, to the following:

Redundancy - The data centers are designed to anticipate and tolerate failure while maintaining service levels with core applications deployed to multiple regions.

- Network Redundancy – internet connectivity has redundant lines at every data center as well as dual line cross data center connectivity.
- Storage replication – service data and configuration are replicated across all hosted data centers to provide uninterrupted service to clients.
- Configuration and metadata backup – is performed to ensure service rapid recovery in case of a disaster.
- Redundant Power – the data center electrical power systems are designed to be fully redundant and maintainable without impact on operations, 24 hours a day, and Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure.
- Data centers use generators to provide backup power for the entire facility.

- Fire Detection and Suppression – Automatic fire detection and suppression equipment have been installed to reduce risk.
- Climate and Temperature Controls – maintain a constant operating temperature and humidity level for all hardware using sensors that report to a remote management system.
- Security Monitoring - In addition, video cameras are installed inside and outside the data centers, provided by the hosting company. Nebius also maintains its own video cameras within the hosted data centers with recordings stored on camera and on external storage.
- Physical access- Nebius recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures, and controls have been implemented to help prevent unauthorized access to data, assets, and restricted areas. Nebius provides physical access to its data centers for approved employees and contractors who have a legitimate business need for such privileges. All visitors are required to be approved before getting access to the data center. Also, cardholder access to data centers is reviewed quarterly. Cardholders marked for removal have their access revoked as part of the review.

Infrastructure Security

Infrastructure security processes include the practice of protecting the underlying hardware, software, networks, and facilities that support the operation of an organization's IT environment. A comprehensive infrastructure security process involves securing physical assets, implementing robust access controls, hardening servers and network devices, and maintaining up-to-date patch management. It also includes network segmentation, intrusion detection and prevention systems (IDPS), firewalls, and continuous monitoring to detect and respond to threats in real time. Security best practices such as principle of least privilege, encryption, and regular audits help ensure that the infrastructure remains resilient against evolving cyber threats. By prioritizing infrastructure security, Nebius can safeguard critical systems and ensure business continuity, such as:

- End-to-End Network Isolation - the Virtual Private Cloud is designed to be logically separated from other cloud customers and to prevent data within the cloud from being intercepted.
- External & Internal enforcement points - All servers are protected by restricted Nebius firewall rules. The configuration of the cloud providers' firewall rules is restricted to authorized personnel.
- Server Hardening - all servers are hardened according to industry's best practices.

Application Security

Application security is a critical component of the software development lifecycle, aimed at protecting applications from threats and vulnerabilities throughout their design, development, deployment, and maintenance. A robust application security process involves identifying security requirements, performing threat modeling, conducting code reviews and vulnerability assessments, and implementing secure coding practices. Automated tools such as static and software composition analysis, along with regular penetration testing, help detect and remediate security issues early. Additionally, integrating security into CI/CD pipelines ensures continuous monitoring and rapid response to new threats. By embedding security at every stage, organizations can reduce risk, protect sensitive data, and maintain user trust.

- Penetration Testing - The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. An external web application penetration test is conducted annually. Critical and High issues are investigated and resolved in a timely manner. High/Critical issues are investigated and dealt with as part of the SDLC process or by any necessary means. A re-test is performed, when necessary, to verify the remediation of the high issues.

- Vulnerabilities Management - Internal vulnerability scanning is performed by the relevant teams using sufficient tools. The Nebius operating systems, web applications, and databases undergo vulnerability scans at least quarterly. When an incident is detected, alerts are sent to relevant stakeholders for investigation and resolution in a timely manner. Vulnerability scans for the source code are performed to identify security issues as part of the SDLC. High/critical issues are remediated.
- Segregation of Customer Data - During each user request, a validation process is performed through encrypted identifiers to ensure that only authorized users gain access to the specific data. Part of Nebius' logical security procedures is to ensure users are segregated from each other. Infrastructure metadata and customer data are replicated for fault tolerance on Nebius' storage system. Additionally, Nebius provides customers with the ability to delete their content. Once successfully removed, the data is rendered unreadable.

Operational Security

The company maintains a structured policy and procedure-driven operational security framework designed to protect its infrastructure, devices, and data from evolving threats. Operational security practices are implemented in accordance with the company's Patch Management Policy, Incident Response procedure, Endpoint Hardening and Controls procedure, and Communication Security and Remote Connection procedure, and are aligned with applicable requirements under ISO/IEC 27001 and HIPAA.

Security Incident Response Management

The company has implemented a formal Security Incident Response procedure to guide its response to security incidents and personal data breaches, in accordance with relevant privacy and regulatory requirements. In the event of a suspected or confirmed physical or electronic incident, engineers are instructed to follow defined procedures. Notifications to customers and legal authorities are made as required by applicable privacy regulations. IT vendors are bound by information security, confidentiality, and privacy obligations as part of their contractual agreements. All incident notifications are escalated to the appropriate personnel and addressed in alignment with the company's established incident response procedures and privacy-related objectives.

Endpoint Protection

All employee devices, including workstations and laptops, are equipped with a centrally managed endpoint protection platform. The platform is configured to receive regular updates and is designed to detect and respond to suspicious activity. If an endpoint agent identifies unusual or malicious behavior, alerts are automatically sent to the Security Operations Center (SOC) for investigation and response. These protections are enforced under the Endpoint Hardening and Controls procedure and support the company's commitment to proactive device-level security.

Business continuity and Disaster Recovery

Nebius' business activities are conducted in an ever-changing competitive environment; therefore, continuity in providing service to customers and availability of business information is crucial. Failure to prepare for disruptive events may expose Nebius to serious financial, legal, and image implications and even impact its business survivability.

This understanding obligates the company to assess the consequences of disaster events.

An emergency may arise as a result of natural disasters (earthquake, flood, storm), technical faults (cyber incident, company infrastructure, computer software, hardware or communications

infrastructure), human factors (human error, strike, internal or external sabotage) and others (such as war, fire, explosion, pollution, pandemic etc.)

Nebius developed Business continuity plan and division business continuity procedures: those are operational / business continuity procedures for responding to a disruptive incident and how it will continue or recover its activities based on the recovery objectives identified in the business impact analysis.

Nebius appointed a BCP representative from each division to lead all business continuity activities. This member will be responsible for implementing this policy and other relevant procedures and coordinating business continuity activities, including relevant reports to the company's management.

in addition, Nebius define disaster recovery plans which are technological and infrastructure recovery guidelines of the information and communications systems that support the critical functions. The DR plans include the recovery sites, and the physical and computerized infrastructures required during an emergency.

Nebius also established a Crisis management team - a senior management team that manages the company's recovery activities. The crisis management team has a dedicated plan which outline the "Chain of command" - a clear chain of command during an emergency state.

Incident Management

Nebius defined incident response plan designed to assist Nebius information security teams during a security incident. Since Nebius holds data, information systems, and equipment, which are sensitive both from a business perspective and in terms of privacy, this plan specify the relevant steps needed to be taken in case of an incident.

According to Nebius information security policies, the company is committed to maintaining the confidentiality, integrity, and availability of the information in our possession.

Prompt and appropriate handling of a security incident that could affect data, information systems, or equipment may minimize the damage and reduce the operational, financial, business, and even reputational impact on the company.

Nebius follows an Incident Management process and procedure that aligns with ISO 27001 and NIST 800-61 standards, ensuring a structured and effective approach to handling security incidents.

The plan objectives are to provide an immediate, effective and skillful response to any unexpected activity involving computer information systems, network, services or databases, to prevent collateral damage and determine the communication between the concerned parties and any systematic action concerning the incident. The IR plan goals are as follows:

- Minimize the damage from security incidents and failures, to monitor and learn from these incidents.
- Define a process for reporting security incidents to other parties involved in this process.
- Define the process and methodology for responding to security incidents.
- Any knowledge gained from information security incidents shall be used to strengthen and improve the existing information security controls.

Deloitte.

CC8.0 Change Management

Software Development Lifecycle (SDLC) Overview

As a provider of Cloud and GPU services, Nebius recognizes the importance of securing its products and services. Nebius follows SSDLC (Secure Software Development Lifecycle) guidelines for developing secure software and cloud environment to ensure that security considerations are integrated into every phase of the software development process from the initial phase of designing a new feature or product and up to the maintenance phase.

The software development lifecycle consists of the following stages:

1. Planning and requirements - ensure that security considerations are integrated into the planning and requirements phase of the software development lifecycle
2. Design - the development teams conduct a technical security design review which results in the creation of security requirements list. During the design phase the teams perform threat modeling to identify and mitigate potential security threats, prioritize risks and define a list of security requirements and controls that should be implemented.
3. Development - Nebius code is developed by secure code best practices in addition to the following security activities:

- Secure environment
- Secure Coding Standards
- Third party software management
- Pipeline security and automated security testing
- Penetration testing

3. Deployment and verification - Developers and security teams shall ensure security development and configuration practices for deployment
4. Release and Maintenance - As part of the release phase, there are additional actions taken to ensure security throughout the product's lifecycle:

- New product introduction or New Feature Introduction (NFI): Ensure security requirements are identified early in the NPI / NFI processes.
- Vulnerability management
- Continuing monitoring
- Logging
- Patch Management
- Incident response

5. Supporting activities such as Regularly Security Awareness Training, external penetration tests (Black box or/and grey box) and utilizing threat intelligence feeds to stay informed about emerging threats and vulnerabilities.

Monitoring the Change Management Processes

Changes that may affect systems are communicated through standardized channels to the different team owners. Changes are documented within the system and approved by authorized employees.

Configuration and Patch Management

The company utilizes a centrally managed configuration management system, including infrastructure-as-code tooling, to enforce predefined configurations and desired patch levels across its servers. Patch management is in process for both company laptops and servers. Security settings are hardened and enforced by procedure and cannot be modified by end users. The system is designed to automatically trigger alerts and initiate remediation actions when configuration or patching deficiencies are identified, as outlined in the Patch Management procedure and System and Network Management procedure.

CC9.0 Risk Mitigation

Database Backup

Nebius implemented backup polies and procedures to ensure data availability and reliability in case of system failure or data loss. the backup strategy includes:
Routine Backups: Backup copies of sensitive and essential information will be performed on a scheduled basis.
Testing and Validation: Backups will be tested regularly to ensure successful data recovery.
Offsite Storage: Backup copies will be stored in a geographically separate, physically secure facility.
Pre-Maintenance Backups: Data backups will be performed immediately before any system upgrade or maintenance activity.
Annual Recovery Testing: Company will test its ability to restore backups at least once per year.
Business Continuity and Disaster Recovery (BCP & DRP)

Restoration

Nebius AI maintains robust procedures to ensure timely restoration of services and data in the event of disruption. The AI cloud is designed with high availability and fault tolerance in mind, supported by automated recovery mechanisms and geographically distributed infrastructure.
In the event of a service degradation or outage, restoration efforts are prioritized based on the criticality of the affected systems and customer impact.
The technical support team, in collaboration with platform engineers and incident response personnel, initiates recovery actions in accordance with predefined incident management and disaster recovery plans.

These restoration capabilities are regularly tested and reviewed to align with business continuity objectives and to meet the Trust Services Criteria for availability and processing integrity.

Disaster Recovery Plan (DRP)

Nebius AI has implemented a comprehensive Disaster Recovery (DR) strategy to ensure the resilience and continuity of its services in the event of a major disruption. The DR program is designed to minimize downtime, protect customer data, and restore critical operations within defined recovery objectives.

The platform leverages geographically distributed infrastructure and automated failover mechanisms to maintain service availability.

Key components of the DR strategy include:

- **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)** targets aligned with business and customer requirements.
- **Regular backups** of customer data and system configurations, stored securely across multiple regions.
- **Automated and manual restoration procedures** for infrastructure, services, and data.
- **Periodic testing** of disaster recovery plans to validate effectiveness and ensure readiness.
- **Incident response coordination** between support, engineering, and operations teams to manage recovery efforts efficiently.

In the event of a disaster, Nebius AI activates its DR protocols to restore services in a prioritized manner, ensuring minimal disruption to customers. The DR plan is reviewed and updated regularly to reflect changes in infrastructure, business operations, and risk landscape.

Vendor Risk Management

All third-party vendors undergo a formal risk assessment and due diligence prior to engagement trough a dedicated TPRM system. This risk assessment includes evaluating their security posture, compliance certifications (e.g., ISO 27001, SOC 2), data handling practices, and contractual obligations related to data protection.

Confidentiality Procedures

Data Classification

- Nebius AI maintains a structured data mapping and classification framework to ensure that all data processed, stored, or transmitted within its platform is appropriately identified, categorized, and protected according to its sensitivity and regulatory requirements.
- Data mapping involves systematic identification of data flows across services, systems, and third-party integrations. This includes documenting the origin, destination, format, and processing context of customer and internal data. The mapping process supports risk assessments, privacy impact analyses, and compliance with data protection regulations.
- Data classification is performed based on predefined categories such as:
- **Public**: Non-sensitive data intended for public access.
- **Internal**: Operational data with limited access within the organization.
- **Confidential**: Sensitive business data requiring restricted access.
- **Restricted**: Highly sensitive, strictly controlled information must be protected with the highest level of security. Due to the potential severe consequences of its disclosure, this data requires the most stringent access controls.
- **Personal Data:** any information relating to an identified or identifiable natural person (data subject'); an identifiable natural person is one who can be identified, directly or indirectly.
- Each classification level is associated with specific handling requirements, including access controls, encryption standards, retention policies, and monitoring protocols. Classification is reviewed periodically and updated as necessary to reflect changes in data usage, regulatory obligations, or business operations.
- This framework ensures that Nebius AI maintains strong data governance and aligns with the Trust Services Criteria for confidentiality and privacy.

Deloitte.

Data Encryption (At Rest & In Transit)

Nebius AI employs strong encryption protocols to protect customer data both at rest and in transit, ensuring confidentiality and integrity in accordance with industry best practices and regulatory requirements.

Encryption at Rest
All customer data stored within the Nebius AI platform is encrypted using robust encryption algorithms. This applies to data stored in databases, object storage, file systems, and backups. Encryption keys are managed through a secure and centralized Key Management System (KMS), which enforces strict access controls and supports key rotation and auditing.

Encryption in Transit
Data transmitted across public and internal networks is protected using Transport Layer Security (TLS) protocols, this ensures that data exchanged between customers, services, and third-party integrations is encrypted and safeguarded against interception or tampering.

These encryption controls are continuously monitored and tested to ensure compliance with the Trust Services Criteria for confidentiality and security.

Access Controls & Authorization

Nebius AI enforces a comprehensive access control framework to ensure that only authorized individuals can access systems, data, and resources based on the principle of least privilege.

Role-Based Access Control (RBAC) is implemented across the platform, assigning permissions based on job responsibilities and operational needs. Access to sensitive systems and data is restricted to designated roles and is subject to approval workflows.

Key components of the access control policy include:

- **User Authentication**: Strong authentication mechanisms, including multi-factor authentication (MFA), are required for access to administrative interfaces and sensitive environments.
- **Access Provisioning & Deprovisioning**: Access requests are reviewed and approved by designated managers. Deprovisioning is automated and triggered by role changes, terminations, or inactivity.
- **Periodic Access Reviews**: Access rights are reviewed on a regular basis to ensure alignment with current roles and responsibilities. Exceptions and anomalies are investigated and remediated.
- **Audit Logging**: All access events are logged and monitored for unauthorized or suspicious activities. Logs are retained in accordance with internal policies and regulatory requirements.
- **Privileged Access Management (PAM)**: Elevated access is tightly controlled and monitored. Temporary access is granted only when necessary and is subject to time-bound constraints.

This layered approach to access control ensures that Nebius AI maintains a secure environment while supporting operational efficiency and compliance.

Deloitte.

Data Retention & Disposal

Nebius AI maintains formal policies and procedures for data retention and secure disposal to ensure compliance with legal, regulatory, and contractual obligations, as well as to support the principles of data minimization and lifecycle management.

Those policies and procedures outline the principles for retaining and disposing of information assets within Nebius, ensuring compliance with legal requirements, industry standards, and best practices for data management.

Data Retention
Customer and internal data are retained only for as long as necessary to fulfill the intended business purpose or as required by applicable laws and regulations. Retention periods are defined based on data classification, service type, and contractual agreements. These periods are documented as follows:

1. **Retention Periods.** Personal data shall be retained for the minimum period necessary to fulfill the purpose for which it was collected.
2. **Disposal Methods.** Personal data shall be disposed of securely, using methods that prevent unauthorized access.
3. **Third-Party Providers.** Nebius uses Filerskeepers, a third-party provider, to manage retention periods and ensure compliance.

Data Disposal
At the end of the retention period or upon customer request, data is securely deleted using industry-standard methods to prevent unauthorized recovery.

Access to data scheduled for deletion is restricted, and disposal activities are logged and monitored to ensure accountability and compliance.

Physical Data Disposal

- Use specialized shredders to physically destroy hard drives, CDs, DVDs, and other storage media, or use a hard drive crusher to deform the device, making it unreadable, or create physical holes in the drive to destroy the platters and make data recovery nearly impossible.
- Securely erase external portable hard drives and SD cards using appropriate tools and methods.
- Paper documents containing personal data should be disposed of using shredding machines or outsourcing to a secure shredding service

Confidential Data Transmission

Nebius AI ensures the confidentiality and integrity of data transmitted across its platform through the use of secure communication protocols and encryption standards. All data in transit, whether between internal services, customer endpoints, or third-party integrations, is protected using encryption mechanisms as specified above.

Transport Layer Security (TLS) is enforced for all external and internal communications. This includes data transmitted via APIs, web interfaces, and service-to-service communications.

Virtual Private Network (VPN) technology is used to secure administrative and operational access to internal systems and environments. VPN connections are encrypted and authenticated,

ensuring that only authorized personnel can access sensitive infrastructure. VPN usage is monitored and governed by access control policies, including multi-factor authentication and session logging.

To further safeguard confidential data Nebius implemented the following controls:

- **Network segmentation and firewall rules** are applied to restrict data flows to only authorized paths.
- **Data integrity checks** are performed to detect unauthorized modifications during transmission.

- **Third-Party Data Handling**

Nebius AI maintains strict controls and oversight over third-party service providers that process, store, or transmit customer data. These controls are designed to ensure that third parties adhere to the same standards of security, confidentiality, and privacy as Nebius AI.

Data Sharing Controls
Nebius defined a dedicated policy which outlines the rules for processing and storing customer business data and customer metadata within the company. Data shared with third parties is limited to the minimum necessary to perform the contracted services. Access is governed by strict contractual agreements, including data processing addendums (DPAs) and confidentiality clauses. Where applicable, data is anonymized or pseudonymized before transmission.

Security & Compliance Requirements
Third parties are required to implement appropriate technical and organizational measures to protect data, including:

- Encryption of data in transit and at rest
- Access controls and authentication mechanisms
- Incident detection and response capabilities
- Regular security audits and assessments

Breach Notification Procedures

In the event of a security incident involving customer data, vendors are required to notify Nebius AI without undue delay within a defined timeframe. This notification must include the nature of the breach, affected data, mitigation steps taken, and any potential impact. Nebius AI coordinates with the vendor to assess the risk, implement remediation measures, and communicate with affected stakeholders as necessary.

Availability Procedures

Production Monitoring

The production environment is logically separated into distinct “Tenants”, each serving as the top-level resource boundary allocated to customers for managing their own cloud resources. Access to each customer’s environment through the web interface is conducted using production accounts managed by the company’s Identity and Authentication (IAM) service, ensuring only relevant users are authorized.
Access to the production environment is protected and restricted. Privileged access to the company’s infrastructure, servers, and production resources is conducted through a VPN connection to the data centers, with each connection uniquely identified at the data center level.

Deloitte.

This access is limited to authenticated and authorized personnel according to their business function via our Single Sign On system.

Support

Nebius AI is committed to delivering reliable and responsive support experience to ensure customers can fully leverage the AI cloud capabilities. Nebius provides a structured support model that includes access to comprehensive technical documentation and a dedicated in-house support team.
Customers can expect responses to support inquiries within 24 hours during business hours aligned with the GMT+1 time zone. The support team consists of experienced engineers who are deeply familiar with Nebius AI and work closely with internal development, product, and R&D teams. This close collaboration ensures that customer feedback is promptly relayed to the relevant stakeholders for continuous improvement.
Support services cover a wide range of needs, including but not limited to access recovery, troubleshooting, service configuration, documentation guidance, incident response, and third-party software integration. For customers requiring more personalized assistance, a dedicated technical account manager is available.

Deloitte.

www.deloitte.co.il

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 244,400 professionals are committed to becoming the standard of excellence.
Brightman Almagor Zohar & Co. (Deloitte Israel) is the member firm of Deloitte Touche Tohmatsu Limited in Israel. Deloitte Israel is one of Israel's leading professional services firms, providing a wide range of world-class audit, tax, consulting, financial advisory and trust services. Through approximately 100 partners and directors and 1000 employees the firm serves domestic and international clients, public institutions and promising fast-growth companies whose shares are traded on the Israeli, US, and European capital markets.