

HITACHI

September 2026

Hitachi Vantara Technical and Organizational Measures

Hitachi Vantara

Our Cybersecurity Program

Hitachi Vantara maintains a comprehensive cybersecurity program designed to protect our operations, products, services, and customer data against evolving threats. The program is built on risk-based governance, secure development practices, continuous monitoring, vulnerability management, incident response, supplier security, data protection, and operational resilience. These capabilities are supported by formal policies, standards, leadership oversight, and continual improvement processes aligned with recognized industry frameworks and regulatory expectations. Through this integrated approach, Hitachi Vantara works to strengthen security, maintain customer trust, and support the reliable delivery of critical digital infrastructure.

Secure Product Development

At Hitachi Vantara, we focus on shifting left across products and services to support alignment with industry standards and security frameworks. We follow a Secure by Design approach aligned with the NIST Secure Software Development Framework (SP 800-218). The company supports the Secure by Design pledge, and product security practices are designed to align with its principles where applicable. Hitachi Vantara also supports the Secure Software Development Attestation requirements associated with Executive Order 14028, “Improving the Nation’s Cybersecurity,” including M-22-18 attestation activities for VSP One families (Block, Object, and File), as applicable.

Secure Development Practices	
Threat Modeling	Structured threat modeling assessments identify potential attack vectors and security risks early in the development lifecycle.
Peer Code Review	Code changes undergo peer review to identify defects, improve software quality, and support adherence to secure coding practices.
Architecture Review	Deep-dive reviews evaluate security-relevant aspects of the solution, including architecture diagrams, cryptographic implementations, protocols, external dependencies, identity management, APIs, interfaces, availability requirements, and system components.
Security Hardening	Products are evaluated against established CIS and STIG benchmarks to identify configuration risks, define secure baseline configurations, and provide hardening recommendations across supported products and components.
Security Testing and Penetration Testing	Hitachi Vantara combines automated security testing with specialist-led manual assessments throughout development and before release. Automated activities include Software Composition Analysis (SCA), Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and infrastructure vulnerability assessments. Together, these activities help identify vulnerable components, coding weaknesses, application vulnerabilities, and infrastructure risks as part of development and release validation. Manual penetration testing is performed by specialists to simulate techniques used by real-world threat actors and identify security weaknesses that may impact business risk. Assessments evaluate areas such as authentication, authorization, session management, input validation, cryptography, business logic, APIs, and other product-specific attack surfaces.

Product and Managed Services Security

Managed Services

Hitachi Vantara cloud and managed services are delivered with enterprise-grade controls and are independently certified or attested against the standards listed below. Certification scope varies by service and location; confirm the applicable scope for each certification in the Certifications & Compliance section of the Trust Center.

- **ISO 27001:** International standard for managing information security risks through a formal Information Security Management System.
- **TISAX:** Automotive industry assessment for information security, focused on protecting sensitive partner and supplier information.
- **SOC 1 Type 2:** Independent audit of controls relevant to financial reporting.
- **SOC 2 Type 2:** Independent audit of security and service controls.
- **ISO 22301:** International standard for business continuity management and organizational resilience.
- **ISO 20000:** International standard for IT service management and consistent delivery of IT services.
- **ISO 9001:** International standard for quality management and continuous improvement of business processes.

Platform Security: Accelerate and protect your critical workloads with VSP One Block

VSP One Block incorporates security capabilities that support compliance with recognized industry standards. Certification scope and assurance level differ by product series.

Product series	Assurance item	Status and scope
VSP One Block 20	<u>FIPS 140-3 Level 1 Management Software Hybrid Firmware</u>	Validated cryptographic modules providing standardized protection of sensitive information.
VSP One Block 20	<u>Common Criteria</u>	Certified against internationally recognized security evaluation standards.
VSP One Block 80	<u>FIPS 140-3 Level 2</u>	Enhanced cryptographic assurance through additional physical and logical security protections.
VSP One Block 80	Common Criteria	Currently in the certification process.

Encryption and Key Management

Hitachi Vantara employs robust encryption mechanisms to support data security across our products and services. Specific encryption functionality varies by product and deployment architecture.

Data at Rest: Hitachi Vantara Storage solutions provide encryption capabilities to protect stored customer data.

Data in Transit: Hitachi Vantara products support TLS 1.3 and TLS 1.2 to protect communications between users, applications, APIs, and management services. Customer-managed certificates are supported.

Certificate Management: Customers can install and manage their own CA-issued certificates, with support for PKI integration and certificate lifecycle management.

Enterprise Cybersecurity and Operational Resilience

Governance and Oversight

Information security governance is embedded at the executive level. Formal policies and standards aligned with ISO/IEC 27001:2022 and NIST are approved and reviewed by management. Senior leadership receives regular reporting on risk posture, control effectiveness, and resilience indicators, including time to detect, time to contain, recovery confidence, and service continuity.

Risk Management

Hitachi Vantara operates a formal, risk-based information security risk management program modeled on ISO/IEC 27005 and NIST guidance. Risks are assessed and treated based on likelihood, exploitability, asset criticality, and potential customer and systemic impact. This includes scenarios where AI-assisted techniques materially compress the time between vulnerability discovery and attempted exploitation. Risk governance focuses on control effectiveness under these conditions rather than reliance on vulnerability secrecy or delayed disclosure. Lessons learned from incidents and threat intelligence, particularly those involving AI-assisted discovery or exploitation techniques, are incorporated into risk assessments, control design, and operational procedures to ensure the ICT risk management framework evolves with the threat landscape.

Vulnerability and Exposure Management

Identification activities address new avenues of exploitation revealed by machine-assisted vulnerability discovery. This includes risks that arise before official disclosure or remediation guidance. Asset criticality and service dependency mapping help assess possible downstream operational impact and help with prioritization.

Hitachi Vantara maintains a vulnerability disclosure and handling process to receive reports from internal and external sources, triage and validate findings, and coordinate remediation. Where appropriate, customers and other stakeholders are notified through security advisories, support channels, and coordinated disclosure practices, with mitigation and patch guidance provided when available.

Continuous vulnerability and exposure management covers enterprise, product, and managed services, with prioritization based on exploitability, threat intelligence, and asset criticality. This approach aims to maintain effective control and governance during rapid discovery periods, rather than predicting or cataloging all vulnerabilities in advance.

Identity and Access Management

Access to systems is restricted to authorized users based on business need. Where supported, attribute-based access controls use identity context and device assurance signals (for example, device binding) to inform access decisions and step-up authentication. Layered identity controls include strong authentication, multifactor authentication, role-based access controls, and privileged access management (PAM) capabilities such as privileged credential vaulting, just-in-time access, approval workflows, privileged elevation, break-glass access, and enhanced monitoring of privileged activity, supported by periodic access reviews. Identity is treated as a primary control plane to limit lateral movement and the propagation of impact across systems, particularly in scenarios where accelerated discovery enables attackers to rapidly chain multiple weaknesses.

Monitoring, Detection, and Response

Hitachi Vantara provides continuous 24/7 monitoring across endpoint, cloud, identity, and network layers, centrally logging and analyzing security events for prompt detection, investigation, and remediation. Detection capabilities are designed to identify anomalous and behavioral indicators of compromise, including activity associated with novel exploitation techniques and previously unseen attack patterns, rather than reliance on known signatures alone.

Response and recovery processes are designed to operate effectively where exploit windows are compressed, and multiple issues may be discovered or exploited concurrently.

Communications and Human Attack Surface Protection

Behavior-based protections are implemented across email and collaboration platforms to detect impersonation, account takeover, and anomalous communication patterns. Domain authentication controls are enforced to prevent unauthorized spoofing of Hitachi Vantara domains.

Incident Management and Operational Resilience

Defined information security incident management processes support timely detection, escalation, containment, recovery, and post-incident review. Business continuity and disaster recovery capabilities are maintained and tested to support ongoing service delivery and regulatory expectations. Communication arrangements support timely, accurate, and proportionate information sharing regarding ICT risks and incidents, including where AI-accelerated discovery materially changes risk exposure or response priorities.

Backup, restoration, and recovery arrangements support resilience in scenarios where accelerated discovery leads to wider or faster-moving disruption, ensuring critical services can be recovered without reliance on prolonged forensic analysis or delayed remediation cycles.

Supplier and Third-Party Security

Risk-based security requirements are applied during supplier onboarding and throughout the supplier lifecycle. Contractual, governance, and monitoring mechanisms define security expectations proportionate to risk and data sensitivity.

Supply Chain Security

Hitachi Vantara operates a controlled global supply chain supported by its own manufacturing and distribution network across Asia-Pacific, China, Europe, and North America. These facilities manage the receipt, storage, configuration, testing, and distribution of storage, compute, and networking hardware, and are certified to recognized international standards for quality, environmental management, and occupational health and safety. Logistics integrity is maintained through established trade and customs controls governing shipment documentation and routing, and the distribution centers participate in recognized trusted-trader supply chain security programs. Product integrity is further supported by Hitachi Vantara's direct control over the development and manufacturing of its storage platforms, which reduces reliance on external components and strengthens assurance across the supply chain.

Business Continuity and Operational Resilience

Hitachi Vantara maintains a Business Continuity Management program aligned to ISO 22301, with executive-level governance and regular management review. The program addresses crisis management, major incident management, IT disaster recovery, and recovery of critical business processes, and the Global Delivery function holds ISO 22301 certification. Infrastructure is designed for redundancy and resilience, with backup and alternate processing arrangements that support continued operations during disruption. Recovery objectives are defined according to the criticality of the business function, and continuity plans are exercised and reviewed on a regular basis to confirm they remain effective.

Data Privacy and Protection

Hitachi Vantara maintains a Global Data Protection and Privacy Policy governing how personal information is collected, processed, used, and transferred, supported by an internal Data Protection Standard that defines minimum requirements for the security, privacy, integrity, and availability of data across its full lifecycle. Customer data is classified as confidential, and authorized personnel may access it only as necessary to deliver the contracted service;

customer data is not disclosed except in accordance with the Data Processing Agreement, written customer instructions, or applicable law. Data protection measures are implemented to support compliance with applicable privacy regulations such as the GDPR and CCPA, and established processes govern data subject rights requests, including access, correction, deletion, restriction, objection, and portability. All personnel complete data protection training on joining and annually thereafter, covering their obligations under company privacy and security policies.

AI Governance and Responsible Use

Hitachi Vantara applies a governed approach to the secure, responsible, and compliant development, acquisition, deployment, and use of AI technologies across both internal business applications and AI-enabled products and services. AI-specific cybersecurity, privacy, regulatory, and ethical considerations are integrated into the broader security and data governance framework, with risk-based review applied throughout the AI lifecycle and human oversight maintained. AI use cases are evaluated through a cross-functional governance model that brings together security, legal, privacy, data, and compliance perspectives and aligns with recognized industry frameworks and guidance for trustworthy and responsible AI.

Assurance, Metrics, and Continuous Improvement

Security metrics, audit outcomes, and improvement actions are reviewed through established governance forums. Findings are tracked and used to drive continual improvement and maintain alignment with evolving regulatory expectations, including UK and EU supervisory frameworks.

Standards and Regulatory Alignment

Hitachi Vantara's security controls are aligned with ISO/IEC 27001:2022, ISO/IEC 27002:2022, the NIST Cybersecurity Framework, the NIST Secure Software Development Framework, OWASP guidance, the EU NIS2 Directive, the EU Cyber Resilience Act (CRA), the Digital Operational Resilience Act (DORA), and others. Alignment does not imply certification or regulatory approval unless explicitly stated for a specific product or service.

HITACHI

f

About Hitachi Vantara

Hitachi Vantara is transforming the way data fuels innovation. A wholly owned subsidiary of Hitachi, Ltd., we're the data foundation the world's leading innovators rely on. Through data storage, infrastructure systems, cloud management and digital expertise, we build the foundation for sustainable business growth.

© Hitachi Vantara LLC 2026. All Rights Reserved.