Anunta's Information Security, Privacy, and Service Management Policy and Program

Ver 3.3

17-Jul-2025

Anunta's Information Security, Privacy, and Service Management Policy and program have been developed in accordance with globally recognized frameworks such as ISO 27001, ISO 27701, ISO 20000, SOC2, PCI DSS, HIPAA, and industry best practices.

Table of Contents

1. **About Anunta** 3
2. **Objective & Scope** 3
3. **Applicability** 4
4. **Roles & Responsibilities** 5
5. **Information Security Policies** 6
6. **Program Activities** 7
   - 6.1. The Information Security & Privacy Program 7
   - 6.2. Information Security & Privacy Awareness, Education and Training 7
   - 6.3. Security and Confidentiality of Customer Information 8
   - 6.4. Protection against Any Anticipated Threats or Hazards to The Security or Integrity of Information 9
   - 6.5. Protect Against Unauthorized Access to Information Assets, PII, or Company Sensitive Information 10
   - 6.6. Sensitive Information Protection and Disposal 11
   - 6.7. Availability of Information for Business Processes 11
   - 6.8. Information Security Awareness and Training Program 11
7. **Deviations and Exceptions** 12
8. **Violations** 12
9. **Definitions** 12
10. **Mapping ISO 27001:2022 to ISO 27701:2019, NIST SP 800-53 R5, PCI-DSS v4 & HIPAA** 13

1. About Anunta

Anunta is a leading Managed Digital Workspace Solution Provider that enables organizations to build secure and scalable digital workspaces on private, public, and hybrid clouds. Anunta's offerings are focused on Desktop-as-a-Service (DaaS), modern desktop management, BYOD, and cloud transformation.

Anunta's Managed DaaS is a fully managed, custom-built DaaS solution for global organizations. It provides on-demand virtual desktops hosted on any public cloud or customer's on-premises infrastructure using Virtual Desktop Infrastructure (VDI) technology. The DaaS offering covers the full DaaS lifecycle support and end-to-end design, onboarding, migration, and management of virtual desktops.

Anunta offers a variety of product portfolio offerings.

- **EuVantage** offers 24/7 infrastructure monitoring.
- **DesktopReady** is a packaged DaaS offering that provides secured, pre-configured virtual desktops that are easy to deploy and use on a public cloud.
- **Cloud Optimal** helps organizations achieve transparency and optimize the cost of their cloud infrastructure.

Anunta is a partner to Top-Tier technology OEMs and cloud providers and has successfully migrated over 600,000+ user desktops to the cloud. Anunta optimizes the design phase to achieve the best TCO outcomes and provide seamless and uninterrupted user migration.

Anunta's mission is to empower end users with high-performing desktops on the cloud that are secure, seamless, and available for business from anywhere. Anunta's vision is to help customers maximize their business potential by providing user-centric digital workspace solutions.

Anunta is certified by ISO 27001, ISO 27701, and ISO 20000 and is a SOC2 Type-2, PCI-DSS & HIPAA compliant organization.

Anunta Technology Management Services Ltd. (ATMSL) is the parent company registered in Mumbai, India, with offices in Mumbai, Chennai, and Bangalore. It consists of the Global Delivery Center (DaaS Operations Team), Business (Sales & Marketing), and other Corporate Support Teams (HR, Finance, Legal, Software Development, Information Security, etc.).

Anunta Technology Inc. (ATI) in the US, Anunta Tech Pte. Ltd. (ATPL) in Singapore, Anunta Technology FZCO (AT FZCO) in the UAE, and Anunta Tech Australia Pty Ltd. (ATAPL) in Australia are subsidiary organizations comprising Business (Sales and marketing) Teams.

Managed DaaS services are delivered from Anunta's Global Delivery Centers in India, and data centers are co-located at Netmagic Solutions, Mumbai, and Chennai.

2. Objective & Scope

Under this policy, 'Company' refers to Anunta Technology Management Services Pvt. Ltd. and all subsidiary brands beneath it.

The Company acknowledges that IT systems, applications, services, and information are valuable assets that are essential to supporting our strategic objectives.

The Company's executive management supports the goals and principles of security in line with the Company's business strategy and objectives. It is committed to the continual improvement of the Information Security Management System.

The Company understands that Information security management is an ongoing cycle of continuous improvement in response to emerging and changing threats and vulnerabilities. This is vital for the continued protection of all information assets and the Company's and its Clients' reputations.

The Company's Information Security, Privacy, and IT Service Management Program objective is to achieve the information security, privacy, and IT service requirements per ISO 27001, ISO 27701, ISO

20000, System and Organization Controls 2 (SOC2) by American Institute of Certified Public Accountants (AICPA), the Payment Card Industry Data Security Standards (PCI/DSS), the US Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST) SP800-53, Cyber Security Framework (CSF), and Center for Internet Security (CIS) Top 20, the US Federal Information Security Modernization Act (FISMA) so that we can meet the compliance obligations within ISO, SOC2, HIPAA, PCI-DSS, DPDP, GDPR, CCPA, FISMA and other applicable standards, Legal, Regulatory, and Client contractual requirements.

The scope of these objectives includes:

- Implementing ISMS, PIMS, and ITSM by adopting relevant ISO/IEC frameworks.
- Maintaining confidentiality, integrity, availability, and privacy of information.
- Managing risks appropriately.
- Meeting regulatory, legislative, and contractual requirements.
- Meeting business and customers' requirements.
- Improving end-user experience.
- Managing business continuity scenarios.
- Ensuring information security and privacy is integral to services delivered and solutions developed.
- Information Security and Privacy violations, weaknesses, and threats – actual or suspected – are reported and investigated.
- Information Security and Privacy Awareness programs are implemented.
- Information Security, Privacy, and Service Management Systems are continually improved.

To support this, we have implemented globally recognized security frameworks and industry best practices to ensure the related Information Security Objectives are fully met, protecting all information assets' confidentiality, integrity, availability, and privacy from internal and external threats.

- **Information Security Management System (ISMS)** based upon the International Standard for Information Security defined by the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2022.
- **Privacy Information Management System (PIMS)** based upon the International Standard for Privacy Information Management requirements defined by the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27701:2019
- **Information Technology Service Management System (ITSM)** based upon the International Standard for Information Security defined by the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 20000-1:2018.
- **Service Organization Controls (SOC2)** based upon Association of International Certified Professional Accountants (AICPA) SOC 2® Trust Services Criteria.
- **PCI/DSS Compliance** based upon Payment Card Industry Data Security Standard.
- **HIPAA Compliance** is based on the Health Insurance Portability and Accountability Act of the US to protect the privacy of individuals' health information (ePHI).

3. Applicability

- **Who** - Employees, consultants, vendors, contractors, and temporary staff who access, use, process, or store the company's information, client data, information, or technology for the company and affiliates.
- **When** - Always.
- **Where** - All company locations.

4. Roles & Responsibilities

Information security is the responsibility of all Company employees/contractors, including the Board of Directors, vendors, affiliates, and service providers. The Company management team actively supports the maintenance of adequate technical and procedural safeguards and has organized information security responsibilities to implement and monitor this program appropriately.

- **Board of Directors (Board) and Executive Management (C-Suite)** – The Board has delegated to the CEO and executive management to provide oversight of the Company's Information Security Program and related Policies. This allows the management to fulfil the requirements of all interested parties and ensure continual improvement. The Executive Team shall ensure that the systematic review of the performance of the Information Security Program is conducted regularly to ensure that all objectives are being met and that any issues identified through the audit program and management processes are remediated promptly.
- **Senior Leaders** – Responsible for overseeing and managing the Information Technology-related procedures, processes, and standards used to enforce, monitor this program, and ensure implementation of the policy requirements.
- **Chief Information Security Officer (CISO)** – Responsible for implementation and monitoring of this Policy, including but not limited to (1) Ensuring that the implementation of information security controls and policies is coordinated across each business unit at the Company; (2) Monitoring the overall compliance to security policies; (3) Initiating plans to maintain security training and awareness; (4) Addressing and responding to information security exceptions, incidents, and non-compliance of information security policies.
- **Data Protection Officer (DPO)** – Responsible for (1) Reviewing and monitoring policy violations and recommending appropriate corrective or disciplinary actions in privacy-related matters, (2) Ensuring Anunta processes Personal Data of the PII Principle in compliance with the applicable data protection rules, (3) Uphold data protection laws and practices and Monitor compliance (4) Support business operations at Anunta and data handling (5) Notify teams and authorities of data breaches (6) Review and approve the privacy policy (7) Review privacy impact assessments (8) Approve exceptions to this policy (9) Initiate appropriate actions against defaulters
- **HIPAA Compliance Officer (HCO)** – Responsible for (1) developing and implementing compliance programs, (2) developing and delivering training programs, (3) monitoring and reviewing HIPAA compliance, (4) conducting risk assessments and identifying potential vulnerabilities, (5) Incident response, and (6) reporting to stakeholders, among others
- **General Counsel/Legal** – Responsible for providing management oversight of the insurance purchasing process. Communicates with relevant business units to ensure insurance coverage meets business needs. In addition, it provides management oversight of the Company's contracts with customers and third parties to minimize security risks.
- **Security Control Owners (Accountable)** – Ensure the required processes and procedures are in place to implement the Security Control requirements through effective delegation and oversight. Ensure evidence of the implementation is provided during Audits, and attend Audits or delegate when requested.
- **Information Asset Owners (IAOs)** – Identify their information assets and areas of responsibility. Know the business purpose and use of the Information assets. Complete the Information Asset Register (IAR) and ensure it is maintained.
- **System Owners** – Ensure that access to IT systems or networks in their scope is only available to authorized personnel. All approvals and checks are obtained before approval, such as from the Line Manager, Information Asset Owner, Department Owner, etc., and have the required level of Security Clearance and business justification for access to the System and/or Information Assets regarding access requested. Access Audits are conducted in line with policy requirements.
- **Human Resources (HR) Department** – Responsible for exercising hiring and terminating practices securely and appropriately, and ensuring appropriate disciplinary actions are taken when information security policy is violated.
- **Managers (including Officers and department Managers) are responsible** for their business unit's compliance with this Policy and ensuring their business units and staff comply with the security requirements.

- **Company Employees** – Responsible for complying with this Policy and all related information security policies.

5. Information Security Policies

Information Security	▪ To provide management direction and support for information security per business requirements and relevant laws.
Privacy & Protection of PII	▪ To provide management direction and support for privacy & protection of PII per business requirements and relevant laws & regulations.
Organization of Information Security, Privacy, and Service Management	▪ To establish a management framework to initiate and control the organization's implementation and operation of information security. ▪ Maintain contact with appropriate authorities. ▪ To ensure the security of teleworking and the use of mobile devices.
People	▪ To ensure that employees and, where relevant, contractors have undertaken appropriate background verification checks, which shall be carried out per applicable laws and regulations. ▪ To ensure that employees and contractors know and will comply with their information security responsibilities. ▪ To protect the organization's interests while changing or terminating employment. ▪ All employees of the organization shall receive appropriate awareness education and training.
Asset Management	▪ To identify organizational assets and define appropriate protection responsibilities. ▪ To ensure that information receives appropriate protection (at rest & in motion) per its importance to the organization. ▪ To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.
Access Control	▪ A defined user access provisioning process shall be implemented to assign or revoke access rights to all systems and services for all user types. ▪ To ensure authorized user access and to prevent unauthorized access to systems and services. ▪ To make users accountable for safeguarding their authentication information. ▪ To prevent unauthorised access to systems and applications.
Cryptography	▪ Define, implement, and manage cryptographic controls that align with security best practices for applicable data. ▪ All cryptographic keys that are used shall be controlled securely.
Physical and Environmental Security	▪ To prevent unauthorized physical access, damage, and interference to the organization's information and information processing facilities. ▪ To prevent loss, damage, theft, or compromise of information assets and Interruption to the organization's operations.
Technology	▪ Define and establish secure practices for managing and mitigating Information Technology computing assets and end-users from malware. ▪ Implement and manage logs for the organization that ensure that critical system security events are adequately identified, monitored, managed, and retained for at least 90 days. ▪ Establish a vulnerability management program that can adequately identify, categorize, manage, and remediate technical vulnerabilities that can impact the organization.
Communications Security	▪ Effective means to ensure that all network-based communication channels that transfer data internally and externally will be adequately protected. ▪ Provide a safe and secure network environment.
System Acquisition, Development, & Maintenance	▪ Establish the mechanisms and procedures for the secure development and management of organizational software and systems that must be followed.

Supplier Relationships	▪ Ensure third parties or suppliers who interact, manage, maintain, or utilize Company resources and information assets can protect the confidentiality, integrity, and availability of the Company information.
Threat Intelligence	▪ Ensure a framework for collecting, analysing, and using threat intelligence is established and operationalized to protect the organization's information assets from various threats.
Information Security Incident Management	▪ Identify, respond, protect, and resolve incidents for the organization.
Information Security Aspects of Business Continuity	▪ Operationally effective means to ensure the availability and integrity of organizational services from the effects of major failures, disruptions, or disasters must be followed and tested periodically.
Compliance	▪ A compliance program that measures the organization's compliance with the security policies and applicable laws and regulations must be in place. ▪ An effective privacy program that adequately protects the privacy of the Company employees, partners, and network participants must be followed.

***Note**: Policies will be communicated to employees and relevant external parties in a form that is relevant, accessible, and understandable to the intended recipient.*

6. Program Activities

6.1. The Information Security & Privacy Program

The program is designed to establish information security & privacy controls essential to the overall safety and soundness of the Company based on a set of sound principles and policies. The Information Security & Privacy Program defines the framework for managing cyber risk, protecting information, and supporting the proper functioning of information IT resources. The Program will be risk-based and contain administrative, technical, and physical safeguards using a layered approach of preventative, detective, and corrective controls to provide maximum protection and assist in complying with applicable legal and regulatory requirements. The Program's effectiveness must be assessed annually, and results must be reported to the Board of Directors. (NIST PM, ISO A5)

6.2. Information Security & Privacy Awareness, Education and Training

All employees, and where relevant, temporary employees, contractors, and consultants must receive appropriate security & privacy awareness education periodically. (NIST AT, ISO A6 & Clause #7).

The CISO, DPO, and HCO shall implement a security & Privacy awareness training program to promote employee awareness about requirements from ISO 27001, ISO 27701, ISO 20000, PCI DSS, and HIPAA common risks related to information security & privacy practices, company policies/procedures, and their roles and responsibilities to protect information and report incidents. Assessments will be carried out, and metrics will be obtained to monitor the effectiveness of the security awareness program in effectively influencing information security behaviour and assessing employees' adherence to the Company's security policies and procedures.

At a minimum, information security training will cover:

- The Management's commitment to information security throughout the organization.
- The requirement that employees, temporary employees, contractors, and consultants become familiar with and comply with applicable information security rules and responsibilities as defined in the various information security policies, procedures, standards, and agreements, as well as relevant laws, regulations, and contractual obligations.
- Personal accountability for one's actions and inactions in securing and protecting information belonging to the Company and external parties.

- Basic information security procedures (information security incident and potential phishing reporting) and baseline controls (password security, physical security).

6.3. Security and Confidentiality of Customer Information

Area	Control
Encryption	The data in transit is encrypted with TLS 1.2 and above versions. The data at rest is encrypted with AES-256 (Advanced Encryption Standard). (NIST SC & SI, ISO A8)
User Endpoint Encryption	All the Company-issued endpoints are encrypted using BitLocker Advanced Encryption Standard (AES), which has an encryption algorithm with a key.
Database Encryption	All structured databases processing sensitive data are encrypted. (NIST SC & SI, ISO A8)
Wireless Encryption	Wireless communications are carried out with WPA3 (Wi-Fi Protected Access 3), WPA2 (Wi-Fi Protected Access 2, TLS (Transport Layer Security), AES (Advanced Encryption Standard), and IPsec (Internet Protocol Security), encrypting network traffic at the IP layer. Site-to-Site VPNs for secure remote access. A Secure Gateway with MFA for authentication and transmission. (NIST SC & SI, ISO 8)
E-mail Encryption	Confidential data is encrypted when transmitted across public or untrusted networks, and secure e-mail (TLS) is used for communication. (NIST SC & SI, ISO A8)
Network Encryption	All network connections are encrypted over untrusted networks. TLS (Transport Layer Security), AES (Advanced Encryption Standard), and IPsec (Internet Protocol Security) encrypt network traffic at the IP layer. Site-to-Site VPNs for secure remote access. A Secure Gateway with MFA for authentication and transmission. All administrative traffic will be encrypted where feasible. (NIST SC & SI, ISO A8)
Network Segregation	Enforcing ACLs on VLANs and DMZs segregates the networks. Development, Production, and CDE networks are isolated.
Social Engineering Test	Social engineering tests are periodically conducted to assess user awareness and the effectiveness of the security training program. (NIST SI, ISO A8)
Device Control	Device control prevents unauthorized devices from being attached to the network. (NIST CM & SC, ISO A5 & A8)
User Endpoint Control	User endpoint control prevents unauthorized access data leakages via USB & Bluetooth file transfers and protects against malware and malicious behaviour (NIST CM & SC, ISO A5 & A8)
Access Control	Access control prevents unauthorized access to confidential information. (NIST SC & SI, ISO A5)
Vulnerability Management	Internal VAPT, External VAPT, ASV Scan, Wireless network Scan, Segmentation PT, Firewall Security Compliance and Rule Review, Web Application PT, and Secure Code Assessment programs are conducted at a defined frequency to identify potential vulnerabilities on devices, applications, and databases. (NIST SC & SI, ISO A8)
Firewall	A firewall is in place to monitor and block malicious activity and policy violations. (NIST SC, ISO A8)

Incident Handling	An incident response plan is developed to promptly and effectively address security breaches, data leaks, or other incidents. (NIST CP & IR, ISO A5)

6.4. Protection against Any Anticipated Threats or Hazards to The Security or Integrity of Information

Area	Control
Asset Management	An IP-based scanning process is used to identify all endpoints connected to the network. (NIST CM, ISO A5)
Secure SDLC	The Company performs static and dynamic application vulnerability assessments and periodic penetration testing at most twice a year. (NIST CM & SA & SC & SI, ISO A8)
Change Management	A formal change management and secure SDLC process is in place to request, document, and approve changes. (NIST CM, ISO A8)
Data Backup and Restoration	Critical data files are backed up to minimize loss in the event of a system failure or other disaster, and restoration testing is performed periodically to check the data backup. (NIST CP & MP, ISO A8)
Malware Control	Next-generation anti-virus and anti-malware tools (EDR) are deployed on all systems (workstations and servers) and updated dynamically. (NIST SC, ISO A8)
Log Management	A centralised Log Management tool to ingest security events from the critical devices and automated rules to detect suspicious behaviour
Security Event Monitoring	The centralised Log Management tool and Next-generation anti-virus and anti-malware tools (EDR) detect suspicious activity, threats, anomalous behaviour, lateral movements, and other unusual access patterns. Automated email alerts are generated to investigate and mitigate critical and high-severity issues. The SOC team monitors, analyses, and responds to the security events. (NIST AU & IA & SC & SI, ISO A5)
URL Filtering	URL filtering dynamically updates malicious URLs to block uncategorized URLs. (NIST AC & SC, ISO A8)
Firewall Rules	Implement firewalls to protect the internal network and sensitive data. Information Security audits and verifies firewall rules biannually to ensure they are properly configured. (NIST AC & SC, ISO A8)
Attack Surface, Darknet, and Brand Monitoring	The external attack surface, darknet, and brand monitoring are in place to detect issues that threat actors can exploit, validate the issues detected, and act on the threats found during the analysis. (NIST AU & IA & SC & SI, ISO A5)
Threat Intelligence	Information about security and privacy threats is collected and analysed to produce threat intelligence and act on applicable threats. (NIST AU & IA & SC & SI, ISO A5)

6.5. Protect Against Unauthorized Access to Information Assets, PII, or Company Sensitive Information

Area	Control
User Access	Formal processes for employee onboarding and offboarding are in place to provide access to information based on role or re-evaluate access after a job transfer. (NIST AC & IA, ISO A5)
Access Review	Business units and identity access management process owners review a complete and accurate list of users (applications, network access, privileged accounts, databases, shared folders) on an approved schedule to verify that only authorized users have access and that their access rights are appropriate. (NIST AC & IA, ISO A5)
Inactive User Access Review	An automated email with details of inactive IDs is sent out on an approved schedule. Identity access management process owners review the list with business units to delete inactive user IDs. (NIST AC & IA, ISO A5)
Physical Access	Proximity controls are in place at the Company, and access reviews are performed periodically. Data centres also include proximity and visitor monitoring controls. (NIST AC & PE, ISO A5)
Inactive Workstations	Display turnoff or automatic session logout is activated after 5 minutes of inactivity for all workstations. (NIST SI, ISO A8)
Network Monitoring	The network team monitors access to the Company network for unauthorized or unusual activity. (NIST SC, ISO A8)
Passwords	Users' identities (local and remote) are authenticated onto the network and applications using Active Directory accounts, long and complex passwords, and multifactor authentication. Measures are in place to eliminate commonly used weak or compromised passwords. (NIST AC & IA & SC & SI, ISO A8)
Multi-factor Authentication	Multi-factor authentication and secure encrypted connections allow remote network access to critical systems. (NIST AC & IA, ISO A8)
Privileged / Service Accounts	Privileged access rights are based on the minimum requirement for their functional role. Privilege identity is established using the Privilege Identity Management tool. Service accounts are restricted for interactive logon. Privileged account passwords are stored and accessed using a password vault. The team ensures that vendor-provided default passwords are changed for all systems before going into production. (NIST AC & IA, ISO A8)
Network Segregation	Production and non-production environments are segregated to prevent unauthorized access to or changes (NIST SC, ISO A8).
Background Checks	Mandatory background checks are performed for all employees, direct consultants, and third-party employees (contractor employees) before granting access to any Company systems. (NIST PS, ISO A6)
Non-Discloser Agreement	Non-Disclosure Agreements are maintained with all vendors and third parties who access the Company's informational assets. (NIST CP&IR, ISO A5)

6.6. Sensitive Information Protection and Disposal

Area	Control
Data Minimisation	PII and Sensitive PII data are protected using data minimization techniques such as Data Masking, Anonymization, and pseudonymization (ISO A8)
Data Retention and Deletion	Data is securely retained using controls such as encryption, RBAC, etc., and deleted when no longer required to preserve Confidentiality and Privacy (Capture NIST and ISO reference)
Physical Documents	All non-public physical documents are disposed of in the shredding bins. (NIST MP, ISO A8)
Storage Media / IT Equipment	Data stored in a computer's storage disk or on backup media (external USB Storage media, magnetic tapes, CDs, and DVDs) is destroyed before disposal. Electronic items are disposed of per electronic equipment disposal requirements, and a safe disposal certificate is retained as evidence of proper destruction and disposal. (NIST MP, ISO A7)

6.7. Availability of Information for Business Processes

Area	Control
Business Continuity Plan (BCP)	The Company has an approved BCP that documents strategies and workaround procedures for minimizing process downtime during a significant disruption. (NIST CP, ISO A5 & A8, CIS #3)
Disaster Recovery Plan (DRP)	The Company has an approved DRP that documents strategies, procedures, and key information for recovering applications during a significant technology disruption. (NIST CP, ISO A5 & A8, CIS #3)
BCP Testing	Planned BCP tests are conducted periodically to validate the usability and accuracy of documented strategies and procedures. (NIST CP & IR, ISO A5 & A8, CIS #3)
Redundancies	Critical Information Processing facilities are implemented with redundancy sufficient to meet availability requirements. (NIST CP, ISO A5 & A8, CIS #3)

6.8. Information Security Awareness and Training Program

Area	Control
User Awareness Training	The Company's information security awareness program incorporates and supports the Company's information security policies and procedures and includes mandatory training designed to ensure employees understand and exhibit the necessary behaviors and skills to ensure the organization's security. On-demand training modules are available for employees on the Learning Management System. (NIST AT, ISO A6, CIS #14)
Alerts, Advisories, and Communication	Information security awareness programs also include periodic alerts, advisories, and email communication for all employees. The results of Phishing Simulations are analysed to spread further awareness. (ISO A5 & A6)
Employee Acknowledgment	Employees will acknowledge and sign that they have read and agree to abide by the guidelines outlined in the Information Security Policy. (NIST AT, ISO A6)
User Training Effectiveness	At the end of the training program, an assessment is conducted to evaluate the effectiveness of the Information Security training and awareness. (NIST AT, ISO A6)

7. Deviations and Exceptions

Per Exception Management Policy

8. Violations

Non-compliance with this Policy is considered a serious violation of the Company's business rules and could result in disciplinary and/or legal action up to and including termination of employment.

All employees must acknowledge receipt and confirm that they understand and agree to abide by the rules.

All employees are required to report any non-compliance with this policy to their department manager and the Chief Information Security Officer.

9. Definitions

- **Availability**: Ensuring timely and reliable access to and use of information upon demand by an authorized entity.
- **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity**: Guarding against improper information modification or destruction, ensuring information non-repudiation and authenticity.
- **Information**: Data printed or written on paper, stored electronically, transmitted by post / electronic means, or spoken in conversation.
- **Information Security**: Protect information and IT resources from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
- **Information Security Objectives**: The company's strategic goals and vision contribute to the planned objectives and are added to the Company's Information Security Management System (ISMS) objectives. Failure to meet the objectives may result in failure to meet any of the Company's Visions. The objectives shall be achieved by allocating appropriate resources and delegating responsibility. See the ISMS Manual for further details.
- **Information Security Principles**: This is related to the fundamental principles of Information Security: Confidentiality, Integrity, and/or Availability. The company will additionally refer to principles in some policies to help the reader understand the principles of the requirements set out in the Policy, but in a summarised form. This approach allows the reader to immediately start to consider whether they meet the principles or not.
- **Information Security Program**: The company's framework and practices provide oversight and govern the security of information and IT resources. The Program also describes the program management controls and safeguards to meet information security requirements.
- **IT Resources**: A term broadly describes IT infrastructure, software, and/or hardware with computing and networking capability. These include, but are not limited to, personal and mobile computing devices, mobile phones, printers, network devices, digital video monitoring, data storage and processing systems, electronic and physical media, access tokens, and other devices that may connect to the Company's network.

- **Personally Identifiable Information**: The term "Personally Identifiable Information" (PII) means individually identifiable information about an employee collected and maintained by the company in an accessible form that, if associated, leads to an individual's identity.
- **Confidential (Company Sensitive Information)**: Any information that a reasonable person would recognize as confidential or proprietary, including documents specifically labelled with terms that would suggest the information to be confidential.

10. Mapping ISO 27001:2022 to ISO 27701:2019, NIST SP 800-53 R5, PCI-DSS v4 & HIPAA

ISO/IEC 27001:2022 Requirements and Controls	ISO/IEC 27701:2019	NIST SP 800-53 Revision-5 Controls	PCI DSS v4 Control(s)	HIPAA Control(s)
ISO/IEC 27001 Clauses				
4. Context of the Organization				
4.1 Understanding the organization and its context	5.2.1	PM-1, PM-11	12.1.1, 12.2.1	164.308(a)(1)(ii)(A)
4.2 Understanding the needs and expectations of interested parties	5.2.2	PM-1	12.1.1	164.308(a)(1)(ii)(D)
4.3 Determining the scope of the information security management system	5.2.3	PM-1, PM-9, PM-28	12.1.2	164.308(a)(1)(ii)(A)
4.4 Information Security Management System	5.2.4	PM-1, PM-9, PM-30, PM-31	12.1.3	164.308(a)(8)
5. Leadership				
5.1 Leadership and Commitment		PM-2, PM-3, PM-29	12.1.1	164.308(a)(2)
5.2 Policy		All XX-1 controls	12.1.1, 12.1.2	164.308(a)(1)(i)
5.3 Organizational roles, responsibilities, and authorities		All XX-1 controls, PM-2, PM-6, PM-29	12.1.3, 12.5.1	164.308(a)(2), 164.308(a)(3)(ii)(B)
6. Planning				
6.1 Actions to address risks and opportunities				
6.1.1 General		PM-1, PM-4, PM-6, PM-9	12.2.1	164.308(a)(1)(ii)(A)
6.1.2 Information security risk assessment	5.4.1.2	PM-9, PM-28, RA-3	12.2.1	164.308(a)(1)(ii)(A)
6.1.3 Information Security Risk Treatment	5.4.1.3	RA-7	12.2.1, 12.2.2	164.308(a)(1)(ii)(B)
6.2 Information security objectives and planning to achieve them		PM-1, PM-3, PM-4, PM-6, PM-9, PM-14, PM-28, PM-30, PM-31	12.1.1	164.308(a)(8)
7. Support				
7.1 Resources		PM-3	12.1.4	164.308(a)(2)
7.2 Competence		PM-13	12.6.2	164.308(a)(3)(ii)(B)
7.3 Awareness		AT-2, PS-8	12.6.1	164.308(a)(5)(i)
7.4 Communication		PM-1, PM-15, PM-28, PM-31	12.6	164.308(a)(6)(ii)
7.5 Documented information				
7.5.1 General		All XX-1 controls, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5	12.1.1, 12.3.1	164.312(c)(1)

ISO/IEC 27001:2022 Requirements and Controls	ISO/IEC 27701:2019	NIST SP 800-53 Revision-5 Controls	PCI DSS v4 Control(s)	HIPAA Control(s)
7.5.2 Creating and updating		All XX-1 controls, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5	12.1.2	164.312(c)(1)
7.5.3 Control of Documented Information		All XX-1 controls, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5	12.3.3	164.312(c)(1), 164.308(a)(8)
8. Operation				
8.1 Operation planning and control		CM-3, PL-7, PM-1, SA-1, SA-4	6.4.1, 6.4.2	164.308(a)(7)(i), 164.310(b)
8.2 Information Security Risk Assessment	5.4.1.2	RA-3	12.2.1	164.308(a)(1)(ii)(A)
8.3 Information Security Risk Treatment	5.4.1.3	CA-5, PM-4, RA-7	12.2.1	164.308(a)(1)(ii)(B)
9. Performance evaluation				
9.1 Monitoring, measurement, analysis, and evaluation		CA-1, CA-7, PM-6, PM-31	10.1.1, 10.2.1	164.308(a)(8), 164.312(b)
9.2 Internal audit				
9.2.1 General		CA-2*, CA-7*	12.11	164.308(a)(8)
9.2.2 Internal audit program		CA-1*, CA-2*, CA-2(1)*, CA-7(1)*, PM-31*	12.11	164.308(a)(8)
9.3 Management review				
9.3.1 General		CA-1*, CA-6*, PM-1*, PM-29	12.11.1	164.308(a)(8)
9.3.2 Management review inputs		CA-7*, CA-7(3)*, CA-7(4)*, PM-4*, RA-3*	12.11.1	164.308(a)(8)
9.3.3 Management Review Results		CA-5*, CA-6*, CA-7*, CM-3*	12.11.1	164.308(a)(8)
10. Improvement				
10.1 Continual improvement		PM-1, PM-9, PM-30, PM-31	12.10.1	164.308(a)(8)
10.2 Nonconformity and corrective action		CA-5, PL-2, PM-4, PM-31, RA-7	12.10.1, 12.10.2	164.308(a)(6)(ii), 164.308(a)(8)
ISO/IEC 27001 Annex-A Controls				
A 5 - Organizational controls				
5.1 Policies for Information Security	6.2.1.1 6.2.1.2	All XX-1 controls	12.1.1, 12.1.2	164.308(a)(1)(i)
5.2 Information security roles and responsibilities	6.2.1.2	All XX-1 controls, CM-9, CP-2, PS-7, PS-9, SA-3, SA-9, PM-2, PM-10	12.5.1	164.308(a)(2)
5.3 Segregation of duties	6.3.1.2	AC-5	7.2.3, 7.3.1	164.308(a)(3)(ii)(B)
5.4 Management responsibilities	6.4.2.1	All XX-1 controls, PM-18*	12.1.1	164.308(a)(1)(ii)(D)
5.5 Contact with Authorities	6.3.1.3	IR-6	12.10.1	164.308(a)(6)(i)
5.6 Contact with special interest groups	6.3.1.4	PM-15, SI-5	12.8.2	164.308(a)(8)
5.7 Threat intelligence	Not Available	PM-16, PM-16(1), RA-10	12.2.1, 12.10.5	164.308(a)(1)(ii)(A)

ISO/IEC 27001:2022 Requirements and Controls	ISO/IEC 27701:2019	NIST SP 800-53 Revision-5 Controls	PCI DSS v4 Control(s)	HIPAA Control(s)
5.8 Information security in project management	6.3.1.5	PL-2, PL-7, PL-8, SA-3, SA-4, SA-9, SA-15	6.4.3	164.308(a)(8)
5.9 Inventory of information and other associated assets	6.5.1.1 6.5.1.2	CM-8	2.4, 12.3.3	164.310(d)(1)
5.10 Acceptable use of information and other associated assets	6.5.1.3	MP-2, MP-4, MP-5, MP-6, MP-7, PE-16, PE-18, PE-20, PL-4, SC-8, SC-28	12.3.1, 12.3.2	164.308(a)(3)(ii), 164.310(d)(1)
5.11 Return of assets	6.5.1.4	PS-4, PS-5	12.3.5	164.310(d)(2)(iii)
5.12 Classification of information	6.5.2.1	RA-2	9.1.1, 12.3.1	164.308(a)(3)(ii)(A)
5.13 Labelling of information	6.5.2.2	MP-3, PE-22	9.1.1, 9.8	164.312(a)(2)(i)
5.14 Information transfer	6.10.2.1 6.10.2.2 6.10.2.3	AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, PE-17, PS-6, SA-9, SC-7, SC-8, SC-15	4.2.1, 12.3.1, 12.3.3	164.312(e)(1)
5.15 Access control	6.6.1	AC-1, AC-3, AC-6	7.1.1, 7.2.1, 7.2.2	164.312(a)(1)
5.16 Identity management	6.6.2.1	AC-2, IA-2, IA-4, IA-5, IA-8	8.1.2, 8.2.1	164.308(a)(3), 164.312(d)
5.17 Authentication information	6.6.2.4	IA-5	8.3.1–8.3.6	164.312(d)
5.18 Access rights	6.6.2	AC-2	7.1.2, 7.2.1	164.312(a)(1)
5.19 Information security in supplier relationships	6.12.1.1	SR-1	12.8.1, 12.8.3	164.308(b)(1)
5.20 Addressing information security within supplier agreements	6.12.1.2	SA-4, SR-3	12.8.2, 12.8.5	164.308(b)(4)
5.21 Managing information security in the information and communication technology (ICT) supply chain	6.12.1.3	SR-3, SR-5	12.8.5	164.308(b)(4)
5.22 Monitoring, review, and change management of supplier services	6.12.2.1 6.12.2.2	RA-9, SA-9, SR-6, SR-7	12.8.5, 12.10.5	164.308(a)(1)(ii)(D), 164.308(b)(4)
5.23 Information security for the use of cloud services	Not Available	SA-1, SA-4, SA-9, SA-9(3), SR-5	12.8.5	164.308(b)(4)
5.24 Information security incident management planning and preparation	6.13.1.1	IR-8	12.10.1, 12.10.2	164.308(a)(6)(i)
5.25 Assessment and decision on information security events	6.13.1.4	AU-6, IR-4	12.10.3	164.308(a)(6)(ii)
5.26 Response to information security events	6.13.1.5	IR-4	12.10.4	164.308(a)(6)(ii)
5.27 Learning from Information Security Incidents	6.13.1.6	IR-4	12.10.5	164.308(a)(6)(ii)
5.28 Collection of evidence	6.13.1.7	AU-3, AU-4, AU-9, AU-10(3), AU-11*	10.3.6, 10.7.2	164.312(c)(2)
5.29 Information security during disruption	6.14.1 6.14.2 6.14.3	CP-2, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13	12.10.6	164.308(a)(7)(i)
5.30 ICT readiness for business continuity	Not Available	CP-2(1)*, CP-2(8)*, CP-4*, CP-4(1)*	12.10.6	164.308(a)(7)(ii)(B)
5.31 Legal, statutory, regulatory, and contractual requirements	6.15.1.1	All XX-1 controls, SC-12, SC-13, SC-17	12.1.1	164.308(a)(1)(ii)(C)
5.32 Intellectual property rights	6.15.1.2	CM-10*	12.1.1	164.308(a)(1)(ii)(C)

ISO/IEC 27001:2022 Requirements and Controls	ISO/IEC 27701:2019	NIST SP 800-53 Revision-5 Controls	PCI DSS v4 Control(s)	HIPAA Control(s)
5.33 Protection of records	6.15.1.3	AC-3*, AC-23, AU-9, CP-9, SC-8, SC-8(1) *, SC-13, SC-28, SC-28(1) *	9.4.1, 12.3.3	164.312(c)(1), 164.308(a)(1)(ii)(C)
5.34 Privacy and protection of personally identifiable information (PII)	6.15.1.4	PM-18, PT-1, PT-3, PT-7, CA-9*, CA-3*, PL-2*, PL-8*	3.2.1, 12.1.1	164.502, 164.308(a)(1)(ii)(A), 164.308(a)(3), 164.312(a)(1)
5.35 Independent review of information security	6.15.2.1	CA-2(1)	12.11.1	164.308(a)(8)
5.36 Compliance with Policies, rules, and standards for information security	6.15.2.2	All XX-1 controls, CA-2	12.1.1, 12.11	164.308(a)(1)(ii)(C), 164.308(a)(8)
5.37 Documented operating procedures	6.9.1.1	All XX-1 controls, SA-5	12.1.1, 12.3.1	164.308(a)(1)(ii)(C)
A 6 - People controls				
6.1 Screening	6.4.1.1	PS-3, SA-21	12.7.1	164.308(a)(3)(ii)(A)
6.2 Terms and conditions of employment	6.4.1.2	PL-4, PS-6	12.1.1	164.308(a)(3)(ii)(A)
6.3 Information security awareness, education, and training	6.4.2.2	AT-2, AT-3, CP-3, IR-2, PM-13	12.6.1, 12.6.2	164.308(a)(5)(i)
6.4 Disciplinary process	6.4.2.3	PS-8	12.10.1	164.308(a)(1)(ii)(C)
6.5 Responsibilities after termination or change of employment	6.4.3.1	PS-4, PS-5	8.1.4, 8.1.5	164.308(a)(3)(ii)(C)
6.6 Confidentiality or non-disclosure agreements	6.10.2.4	PS-6	12.1.1	164.308(a)(3)(ii)(A)
6.7 Remote working	6.3.2.2	None	12.3.9	164.312(a)(1), 164.308(a)(1)(ii)(A)
6.8 Information security event reporting	6.13.1.2 6.13.1.3	AU-6, IR-6, SI-2	12.10.5, 10.6.1	164.308(a)(6)
A 7 - Physical Controls				
7.1 Physical security perimeters	6.8.1.1	PE-3*	9.1.1	164.310(a)(1), 164.310(b)
7.2 Physical entry	6.8.1.2	PE-2, PE-3, PE-4, PE-5, PE-16	9.1.2, 9.2.3, 9.4.1	164.310(a)(2)(iii)
7.3 Securing offices, rooms, and facilities	6.8.1.3	PE-3, PE-5	9.1.1, 9.1.2	164.310(b)
7.4 Physical security monitoring	Not Available	AU-6(6)*, PE-3, PE-3(3), PE-6, PE-6(1), PE-6(4)*	9.1.3, 9.2.1	164.310(a)(2)(ii)
7.5 Protecting against physical and environmental threats	6.8.1.4	CP-6, CP-7, PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23	9.1.1, 9.1.2	164.310(a)(2)(i)
7.6 Working in secure areas	6.8.1.5	SC-42*	9.1.1, 9.1.2	164.310(b)
7.7 Clear desk and clear screen	6.8.2.9	AC-11, MP-2, MP-4	9.3.1, 12.3.1	164.310(d)(1)
7.8 Equipment siting and protection	6.8.2.1	PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23	9.1.1	164.310(c)
7.9 Security of assets off-premises	6.8.2.6	AC-19, AC-20, MP-5, PE-17	9.1.2, 12.3.8	164.310(d)(1), 164.312(b)
7.10 Storage media	6.5.3.1 6.5.3.2 6.5.3.3 6.8.2.5	MA-2, MP-2, MP-4, MP-5, MP-6, MP-7, PE-16	9.8.1, 9.9.1–9.9.3	164.310(d)(2), 164.312(c)(1)

ISO/IEC 27001:2022 Requirements and Controls	ISO/IEC 27701:2019	NIST SP 800-53 Revision-5 Controls	PCI DSS v4 Control(s)	HIPAA Control(s)
7.11 Supporting utilities	6.8.2.2	CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PE-15	9.1.1	164.310(a)(2)(i)
7.12 Cabling security	6.8.2.3	PE-4, PE-9	9.1.2	164.310(c)
7.13 Equipment maintenance	6.8.2.4	MA-2, MA-6	9.1.2	164.310(c)
7.14 Secure disposal or re-use of equipment	6.8.2.7	MP-6	9.8.2, 9.9.1–9.9.3	164.310(d)(2)(ii), 164.310(d)(1)
A8 - Technological controls				
8.1 User endpoint devices	6.3.2.1 6.8.2.8	AC-11	2.2.1, 2.2.4, 5.3.2	164.310(d), 164.312(c)(1)
8.2 Privileged access rights	6.6.2.3	AC-2, AC-3, AC-6, CM-5	7.2.2, 7.2.4, 8.2.2	164.308(a)(3), 164.312(a)(1)
8.3 Information access restriction	6.6.4.1	AC-3, AC-24	7.1.1, 7.2.1	164.308(a)(4), 164.312(a)(1)
8.4 Access to source code	6.6.4.5	AC-3*, AC-3(11), CM-5	6.4.2, 7.2.2	164.312(a)(1), 164.308(a)(1)(ii)(C)
8.5 Secure authentication	6.6.4.2	AC-7, AC-8, AC-9, IA-6	8.3.1–8.3.6	164.312(d), 164.312(a)(2)(i)
8.6 Capacity management	6.9.1.3	AU-4, CP-2(2), SC-5(2) *	11.5.1	164.308(a)(1)(ii)(D)
8.7 Protection against malware	6.9.2.1	AT-2, SI-3	5.2.1–5.2.5	164.308(a)(5)(ii)(B)
8.8 Management of technical vulnerabilities	6.9.6.1 6.15.2.3	RA-3, RA-5, SI-2, SI-5	6.3.1, 6.3.2	164.308(a)(1)(ii)(A), 164.308(a)(8)
8.9 Configuration management	Not Available	CM-1, CM-2, CM-2(3)*, CM-3, CM-3(7), CM-3(8), CM-4, CM-5, CM-6, CM-8, CM-9, CM-9(1)*, SA-10	2.2.1–2.2.5	164.308(a)(1)(ii)(D)
8.10 Information deletion	A.7.3.1 A.7.4.5 A.7.4.6 A.7.4.7 A.7.4.8 B.8.3.1 B.8.4.2 B.8.2.5	AC-4(25)*, AC-7(2)*, MA-2, MA-3(3)*, MA-4(3)*, MP-4, MP-6, MP-6(1)*, SI-21	9.8.2, 9.9.1–9.9.3	164.310(d)(2)(ii), 164.312(c)(1)
8.11 Data masking	A.7.4.4 A.7.4.5	AC-4(23), SI-19(4)	3.4.1, 3.4.2	164.312(a)(1), 164.312(e)(1)
8.12 Data leakage prevention	Not Available	AU-13, PE-3(2)*, PE-19, SC-7(10)*, SI-20	3.3.1, 12.10.5	164.312(e)(1), 164.308(a)(1)(ii)(A)
8.13 Information backup	6.9.3.1	CP-9	12.3.1, 12.3.3	164.308(a)(7)(ii)(A), 164.310(d)(2)(iv)
8.14 Redundancy of information processing facilities	6.15.2.1	CP-2, CP-6, CP-7	12.3.3, 11.1.1	164.308(a)(7)(ii)(C)
8.15 Logging	6.9.4.1 6.9.4.2 6.9.4.3	AU-3, AU-6, AU-9, AU-11, AU-12, AU-14	10.1.1–10.7.3	164.308(a)(1)(ii)(D), 164.312(b)

ISO/IEC 27001:2022 Requirements and Controls	ISO/IEC 27701:2019	NIST SP 800-53 Revision-5 Controls	PCI DSS v4 Control(s)	HIPAA Control(s)
8.16 Monitoring activities	Not Available	AC-2(12), AC-17(1), AU-13*, IR-4(13)*, MA-4(1)*, PE-6*, PE-6(3)*, SI-4, SI-4(4)*, SI-4(13)*, SI-4(16)*	10.2.1–10.4.1, 11.5.1	164.312(b), 164.308(a)(1)(ii)(D)
8.17 Clock synchronization	6.9.4.4	AU-8	10.6.2	164.312(b)
8.18 Use of privileged utility programs	6.6.4.4	AC-3, AC-6	7.2.2, 8.2.2	164.312(a)(1), 164.308(a)(3)(ii)(B)
8.19 Installation of software on operational systems	6.9.5.1 6.9.6.2	CM-5, CM-7(4) *, CM-7(5) *, CM-11*	6.4.2, 6.4.3	164.308(a)(1)(ii)(C), 164.312(c)(1)
8.20 Network Security	6.10.1.1	AC-3, AC-18, AC-20, SC-7, SC-8, SC-10	1.2.1, 1.3.1–1.4.4	164.312(e)(1), 164.312(c)(1)
8.21 Security of network services	6.10.1.2	CA-3, SA-9	1.2.1, 1.3.5	164.308(a)(8), 164.312(e)(1)
8.22 Segregation of networks	6.10.1.3	AC-4, SC-7	1.2.1–1.2.4	164.312(c)(1)
8.23 Web filtering	Not Available	AC-4, SC-7, SC-7(8)	1.3.4, 1.3.5	164.312(e)(1)
8.24 Use of cryptography	6.7.1.1 6.7.1.2	SC-12, SC-13, SC-17	3.5.1–3.6.6	164.312(a)(2)(iv), 164.312(c)(1), 164.312(e)(2)(ii)
8.25 Secure development life cycle	6.11.2.1	SA-3, SA-15, SA-17	6.4.1, 6.4.2	164.308(a)(1)(ii)(D)
8.26 Application security requirements	Not Available	AC-3, SC-8*, SC-13	6.4.1–6.4.3	164.308(a)(1)(ii)(C)
8.27 Secure system architecture and engineering principles	6.11.2.5	SA-8	6.4.2	164.308(a)(1)(ii)(D)
8.28 Secure coding	Not Available	SA-4(3)*, SA-8, SA-11(1)*, SA-15(5)*, SI-10	6.4.2	164.308(a)(1)(ii)(C)
8.29 Security testing in development and acceptance	6.11.2.8 611.2.9	CA-2, SA-4, SA-11, SR-5(2) *	6.4.2, 11.3.1–11.3.2	164.308(a)(8)
8.30 Outsourced development	6.11.2.7	SA-4, SA-10, SA-11, SA-15, SR-2, SR-4	12.8.1–12.8.5	164.308(b)(1), 164.308(a)(8)
8.31 Separation of development, test, and production environments	6.9.1.4 6.11.2.6	CM-4(1), CM-5*, SA-3*	6.4.1, 6.4.2	164.308(a)(1)(ii)(C)
8.32 Change management	6.9.1.2 6.11.2.2 6.11.2.3 6.11.2.4	CM-3, CM-5, SA-10, SI-2	6.4.2, 6.5.1	164.308(a)(1)(ii)(C)
8.33 Test information	6.11.3.1	SA-3(2) *	6.4.2	164.308(a)(1)(ii)(D)
8.34 Protection of information systems during audit testing	6.9.7.1	AU-5*	10.7.1	164.308(a)(1)(ii)(D)

***Note**: An asterisk (*) indicates that additional control may be required to satisfy the intent of the NIST control.*

*** This Document Ends Here ***