Anunta Information Security, Privacy and Service Management Policy and Program

Ver 3.1

6-Oct-2023

Anunta's Information Security, Privacy and Service Management Policy & Program has been developed in line with globally recognized frameworks and industry best practices.

Table of Contents

1. Introduction

Anunta Technology Management Services Ltd. is an industry recognized digital workplace transformation technology provider focused on Desktop-as-a-Service (DaaS), Modern Desktop Management, BYOD and Cloud Transformation.

Anunta's Managed DaaS offering is a fully managed custom-built DaaS solution for global organizations and provides on-demand virtual desktops hosted on any public/private cloud 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's Vision: Helping customers maximize their business potential by providing user-centric digital workplace solutions using Desktop-as-a-Service (DaaS).

Anunta's Mission: To empower users with high-performing cloud desktops that are secured, seamless, and available anywhere for business applications.

2. Objective & Scope

Under this policy 'Company' refers to the Anunta Technology Management Services Pvt. Ltd. and all subsidiary brands that sit beneath.

The Company acknowledges that IT systems, Applications, Services, and Information are valuable assets which are essential in supporting our strategic objectives.

To support this, we have put in place globally recognized security frameworks and industry best practices to ensure the related Information Security Objectives are fully met, so protecting the confidentiality, integrity, availability, and privacy of all information assets 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) 27001:2013.
- **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.
- **SOC for Service Organizations** (SOC2) based upon Association of International Certified Professional Accountants (AICPA) SOC 2® Trust Services Criteria.

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

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

The Company's Information Security Program objective is to achieve the information security principles defined in ISO 27001, ISO 27701, National Institute of Standards and Technology (NIST) SP800-53, Cyber Security Framework (CSF), and Center for Internet Security (CIS) Top 20, Federal Information Security Modernization Act (FISMA) so that we can meet the compliance obligations within ISO, SOC2, FISMA, PCI-DSS, DPDP, GDPR, CCPA and other applicable standards. This includes ensuring that we meet all 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.

3. Applicability

- **Who** - Employees, as well as 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** - At all times.
- **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 maintenance of adequate technical and procedural safeguards and has organized information security responsibilities to appropriately implement and monitor this Program.

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 to ensure continual improvement. The Executive Team shall ensure that the systematic review of performance of the Information Security Program is conducted on a regular basis to ensure that all objectives are being met and any issues are identified through the audit program and management processes are remediated in a timely fashion.

Senior Leaders – Responsible for the oversight and management of the Information Technology related procedures, processes and standards that are used to enforce, monitor this Program, and ensure implementation of the policy requirements.

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.

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, provides management oversight of the Company contracts with customers and third parties, to minimize security risks.

Security Control Owners (Accountable) – Ensure the required processes and procedures are in place to ensure implementation of the Security Control related 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 area 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 appropriate approvals and checks are obtained prior to giving the 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 with regards to access requested. Access Audits conducted in line with policy requirements.

Human Resources (HR) Department – Responsible for exercising hiring and terminating practices in a secure and appropriate manner and ensuring appropriate disciplinary actions are taken when information security policy is violated.

Managers (including Officers and Managers of Departments) – Responsible for their business unit's compliance with this Policy and ensures 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 Policy

5.1. Information Security Policy Requirements

Information Security	▪ To provide management direction and support for information security in accordance with business requirements and relevant laws.
Privacy & Protection of PII	▪ To provide management direction and support for privacy & protection of PII in accordance with business requirements and relevant laws & regulations.
Organization of Information Security & Privacy	▪ To establish a management framework to initiate and control the implementation and operation of information security within the organization. ▪ Maintain contact with appropriate authorities. ▪ To ensure the security of teleworking and use of mobile devices.
Human Resources	▪ To ensure that employees and where relevant, contractors have undertaken appropriate background verification checks which shall be carried out in accordance with relevant laws, regulations. ▪ To ensure that employees and contractors are aware of and will comply with their information security responsibilities. ▪ To protect the organization's interests as part of the process of 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 an appropriate level of protection (at rest & in motion) in accordance with 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 for all user types to all systems and services. ▪ 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 unauthorized access to systems and applications.

Cryptography	▪ Define, implement, and manage cryptographic controls for applicable data that align with security best practices. ▪ All cryptographic keys that are used shall be controlled in a secure manner.
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.
Operations Security	▪ Define and establish secure practices for the management and mitigation of Information Technology computing assets and end-users from malware. ▪ Implement and manage logs for the organization that ensures that critical system related security events are adequately identified, monitored, managed, and retained for at least 90 days. ▪ Establish a vulnerability management program for the organization 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 used to 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 confidentiality, integrity, and availability of the Company information.
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 can measure the compliance of the organization to the stated security policies, 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 sound principles and policies. The Information Security & Privacy Program defines the framework to manage cyber risk, protect information and support 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 effectiveness of the Program must be assessed on an annual basis and results reported to the Board of Directors. (NIST PM, ISO #1, #2)

6.2. Information Security & Privacy Awareness, Education and Training

All employees, and where relevant, temporary employees, contractors, consultants must receive appropriate security & privacy awareness education on a periodic basis. (NIST AT, ISO #3 & Clause #7).

The CISO & DPO shall implement a security & Privacy awareness training program designed to promote awareness among employees about common risks related to information security & privacy practices, company policies / procedures and their roles and responsibilities necessary to protect information and report incidents. Assessments will be carried out, and metrics obtained to monitor the effectiveness of the security awareness program to effectively influence information security behaviour and assess employee's 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 applicable laws, regulations, and contractual obligations.
- Personal accountability for one's own 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 at transit and data at rest is encrypted with TLS1.2 and above version. (NIST SC & SI, ISO #6, CIS #3)
Laptop Encryption	All the Company issued laptops are encrypted using BitLocker Advanced Encryption Standard (AES) as its encryption algorithm is with key.
Database Encryption	All structured databases processing sensitive data is encrypted. (NIST SC & SI, ISO #6, CIS #3)
Wireless Encryption	Wireless communications are carried out with encrypted SFTP, Site-to-site VPN for file transfer, NetScaler Secure Web Gateway with 2FA for authentication and transmission. (NIST SC & SI, ISO #6 & #9, CIS #3)
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 #6 & #9, CIS #3)
Network Encryption	All network connections are encrypted over untrusted networks. All administrative traffic will be encrypted where feasible. (NIST SC & SI, ISO #6 & #9, CIS #3)
Social Engineering Test	Information Security conducts social engineering tests on a periodic basis to assess user awareness and the effectiveness of the security training program. (NIST SI, ISO #8, CIS #14)
Device Control	Device control prevents unauthorized devices to be attached to the network. (NIST CM & SC, ISO #4, CIS #1 & #2)
Access Control	Access control prevents unauthorized access to confidential information. (NIST SC & SI, ISO #6, CIS #6)

Vulnerability Scanning	Information Security utilizes a vulnerability scanning tool to identify potential vulnerabilities on servers on a defined frequency. (NIST SC & SI, ISO #8, CIS #7)
Firewall	A firewall is in place to monitor, block malicious activity and policy violations. (NIST SC, ISO #9, CIS #12)
Incident Handling	Incident response plan is developed to address security breaches, data leaks, or other incidents promptly and effectively. (NIST CP & IR, ISO #12 #13, CIS #17)

6.4. Protection against any anticipated threats or hazards to the security or integrity of information

Area	Control
Asset Management	IP based scanning process to identify all endpoints connected to the network. (NIST CM, ISO #4, CIS #1 & #2)
Secure SDLC	Currently, the Company performs static and dynamic vulnerability assessments of applications, and perform periodic penetration testing, but no less than twice a year. (NIST CM & SA & SC & SI, ISO #10, CIS #4)
Change Management	A formal change management and secure SDLC process is in place to request, document, and approve changes to assets. (NIST CM, ISO #8, CIS #4)
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 on the periodic basis to check the data backup. (NIST CP & MP, ISO #13, CIS #3)
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 #8, CIS #10)
Security Monitoring/Review	Suspected suspicious activity, threats, anomalous behaviour, lateral movements, and other unusual access patterns are detected by next generation anti-virus and anti-malware tools (EDR). Automated email alerts are generated for critical & high severity issues for investigation and mitigation. (NIST AU & IA & SC & SI, ISO #8, CIS #6)
URL Filtering	URL filtering dynamically updates malicious URLs to block uncategorized URLs. (NIST AC & SC, ISO #5 & #9, CIS #12 & 13)
Firewall rules	Implement firewalls to protect internal network and sensitive data. Information Security audits and verifies firewall rules at least bi-annual to verify they are properly configured. (NIST AC & SC, ISO #5 & #9, CIS #12 & 13)
Attack surface monitoring	External attack surface monitoring and brand monitoring are in place to validate, and actions will be taken on the treats found during the analysis. (NIST AU & IA & SC & SI, ISO #8, CIS #13)

6.5. Protect against unauthorized access to Information Assets, PII, or Company Sensitive Information

Area	Control
User Access	Formal processes for employee onboarding and off boarding is in place to provide access to information based on role or re-evaluate access after a job transfer. (NIST AC & IA, ISO #5, CIS #6)
Access Review	Business units along with identity access management process owners review a complete and accurate list of users (applications, network access, privileged

	accounts, databases, shared folder) on an approved scheduled basis to verify only authorized users have access, their access rights are appropriate. (NIST AC & IA, ISO #5, CIS #6)
Inactive User Access Review	An automated email with 60-day inactive IDs is sent out on an approved scheduled basis. Identity access management process owners review the list with business units to delete user IDs who have been inactive for a period of 60 days. (NIST AC & IA, ISO #5, CIS #6)
Physical Access	Proximity controls are in place at the Company. Access reviews are performed on a periodic basis. Data centres include proximity and visitor monitoring controls. (NIST AC & PE, ISO #7, CIS #6)
Inactive Workstations	Display turnoff or automatic session logout is activated after a period of inactivity for all workstations. (NIST SI, ISO #8, CIS #6)
Network Monitoring	Network team monitors access to the Company network for unauthorized or unusual activity. (NIST SC, ISO #9, CIS #12 & #13)
Background Checks	Mandatory background checks are performed for all employees, direct consultants, and third-party employees (contractor employees) prior to granting access to any of the Company systems. (NIST PS, ISO #3)
Passwords	The identity or users (local and remote) is 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 #5 & #8, CIS #6)
Multi-factor Authentication for Remote Access	Multi-factor authentication and secure encrypted connections are in place for remote network access to critical systems. (NIST AC & IA, ISO #5 & #8)
Privileged / Service Accounts	Privilege Access rights are based on the minimum requirement for their functional role. Privilege identity is established using Privilege Identity Management tool. Service accounts are restricted for interactive logon. Privilege Account passwords are stored and accessed using a password vault. Team ensures that vendor provided default passwords are changed for all systems prior to going into production. (NIST AC & IA, ISO #5 & #8, CIS #6)
Environment Segregation	Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (NIST SC, ISO #9.)
Non-Discloser Agreement	Non-Discloser Agreements are maintained with all the vendors and the third party who access the Company informational asset. (NIST CP&IR, ISO#13, CIS #15)

6.6. Disposal of Sensitive Information

Area	Control
Physical documents	All non-public physical documents are disposed of in the shredding bins. NIST MP, ISO #4
Storage Media / IT Equipment	Data stored in a computer's storage disk or on back-up media (external USB Storage media, magnetic tapes, CDs, and DVDs) are destroyed prior to disposal. Electronic items are disposed per electronic equipment disposal requirements and certificate of safe disposal is retained as evidence of proper destruction and disposal. (NIST MP, ISO #4)

6.7. Availability of Information for Business Processes

Area	Control
Business Continuity Plan (BCP)	The Company has an approved BCP which documents strategies and workaround procedures to minimize process downtime during a significant disruption. (NIST CP, ISO #13, CIS #3)
Disaster Recovery Plan (DRP)	The Company has an approved DRP which documents strategies and procedures, and key information to recover applications in the event of a significant technology disruption. (NIST CP, ISO #13, CIS #3)
BCP Testing	Planned BCP tests are conducted on a periodic basis to validate the usability and accuracy of documented strategies and procedures. (NIST CP & IR, ISO #12 & #13, CIS #3)

6.8. Information Security Awareness and Training Program

Area	Control
User Awareness Training	The Company information security awareness program incorporates and supports the Company information security policies and procedures and includes mandatory training which are designed to ensure employees understand and exhibit the necessary behaviours and skills to ensure the security of the organization. (NIST AT, ISO #3, CIS #14)
Employee Acknowledgment	Employees will acknowledge and sign that they have read and agree to abide by the guidelines set forth in the Information Security Policy on an annual basis. (NIST AT, ISO #3, CIS #14)
User Training Effectiveness	At end of training program assessment is conducted to evaluate the effectiveness of the Information Security training and awareness. (NIST AT, ISO #3, CIS #14)

7. Deviations and Exceptions

Per Exception Management Policy

8. Violations

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

All employees are required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder.

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 and includes ensuring information non-repudiation and authenticity.

Information: Data, which is printed or written on paper, stored electronically, transmitted by post / electronic means, or spoken in conversation.

Information Security: The protection of information and IT resources from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.

Information Security Objectives: The strategic goals and vision of the Company contribute to the planned objectives and are added to the Company's Information Security Management System (ISMS) objectives, and significant failure to meet the objectives may result in failure to meet any one of the Company's Vision. The objectives shall be achieved by allocation of appropriate resources and delegation of responsibility. See the ISMS Manual for further details.

Information Security Principles: This is related to the fundamental principles of Information Security being Confidentiality, Integrity and/or Availability. The company will additionally refer to principles in some policies to also 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: Framework and practices established by the Company is to provide oversight and govern the security of information and IT resources. The Program also describes the program management controls and safeguards in place to meet information security requirements.

IT Resources: A term that 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 which 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 together, lead to individual's identity.

Confidential (Company Sensitive Information): Any information which a reasonable person would recognize as being confidential or proprietary, including documents specifically labelled with terms that would suggest the information to be confidential.

10. Appendix 1: Controls Mapping

10.1. CIS Top Critical Security Controls v/s NIST SP 800-53, ISO 27001 and SOC2

CIS Critical Security Control	Description	NIST SP 800-53	ISO-27701	SOC2
Critical Security Control #1: Inventory and Control of Enterprise Assets	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.	CM, SA	#4, #10	CC6.1
Critical Security Control #2: Inventory and Control of Software Assets	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.	CM, SA	#4, #10	CC6.1

Critical Security Control #3: Data Protection	Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.	MP, SA, SC, SI	#5	CC6.1
Critical Security Control #4: Secure Configuration of Enterprise Assets and Software	Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications)	CM, SC, SI	#6, #8	CC6.8
Critical Security Control #5: Account Management	Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.	AC, AU, IA	#4, #5	CC4.1
Critical Security Control #6: Access Control Management	Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.	AC, IA,	#4, #5	CC6.3
Critical Security Control #7: Continuous Vulnerability Management	Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.	SC, SI	#8	CC7.1
Critical Security Control #8: Audit Log Management	Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.	AC, AU, IA	#8	CC7.1
Critical Security Control #9: Email and Web Browser Protections	Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behaviour through direct engagement.	SC, SI	#8, #9	CC6.1
Critical Security Control #10: Malware Defences	Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.	SC, SI	#8, #9	CC6.8
Critical Security Control 11: Data Recovery	Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.	CP, MP	#13	A.1.3
Critical Security Control #12: Network Infrastructure Management	Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.	CM, SA, SC, SI	#8, #9	CC6.1
Critical Security Control #13: Network Monitoring and Defence	Operate processes and tooling to establish and maintain comprehensive network monitoring and defence against security threats across the enterprise's network infrastructure and user base.	SC, SI	#6, #9	CC6.6
Critical Security Control #14: Security Awareness and Skills Training	Establish and maintain a security awareness program to influence behaviour among the workforce to be security conscious and properly	AT	#3	CC2.2

	skilled to reduce cybersecurity risks to the enterprise.			
Critical Security Control #15: Service Provider Management	Develop a process to evaluate service providers who hold sensitive data or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.		#13	CC1.1
Critical Security Control #16: Application Software Security	Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.	SA, SC, SI	#10	CC6.8
Critical Security Control #17: Incident Response and Management	Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.	CP, IR	#12, #13	CC7.4
Critical Security Control #18: Penetration Tests and Red Team Exercises	Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.	SC, SI	#8	CC4.1

10.2. ISO/IEC 27001 Requirements & Controls v/s NIST SP 800-53

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS
ISO/IEC 27001 Requirements	
4. Context of the Organization	
4.1 Understanding the organization and its context	PM-1, PM-11
4.2 Understanding the needs and expectations of interested parties	PM-1
4.3 Determining the scope of the information security management system	PM-1, PM-9, PM-28
4.4 Information security management system	PM-1, PM-9, PM-30, PM-31
5. Leadership	
5.1 Leadership and commitment	PM-2, PM-3, PM-29
5.2 Policy	All XX-1 controls
5.3 Organizational roles, responsibilities, and authorities	All XX-1 controls, PM-2, PM-6, PM-29
6. Planning	
6.1 Actions to address risks and opportunities	
6.1.1 General	PM-1, PM-4, PM-6, PM-9
6.1.2 Information security risk assessment	PM-9, PM-28, RA-3
6.1.3 Information security risk treatment	RA-7
6.2 Information security objectives and planning	PM-1, PM-3, PM-4, PM-6, PM-9, PM-14, PM-28, PM-30, PM-31
7. Support	
7.1 Resources	PM-3
7.2 Competence	PM-13
7.3 Awareness	AT-2, PS-8

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS
7.4 Communication	PM-1, PM-15, PM-28, PM-31
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
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
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
8. Operation	
8.1 Operation planning and control	CM-3, PL-7, PM-1, SA-1, SA-4
8.2 Information security risk assessment	RA-3
8.3 Information security risk treatment	CA-5, PM-4, RA-7
9. Performance evaluation	
9.1 Monitoring, measurement, analysis, and evaluation	CA-1, CA-7, PM-6, PM-31
9.2 Internal audit	CA-1, CA-2, CA-5, CA-7, PM-4
9.3 Management review	CA-6, PM-1, PM-4, PM-9, PM-10, PM-29
10. Improvement	
10.1 Nonconformity and corrective action	CA-5, PL-2, PM-4, PM-31, RA-7
10.2 Continual improvement	PM-1, PM-9, PM-30, PM-31
ISO/IEC 27001 Controls	
A.5 Information Security Policies	
A.5.1 Management direction for information security	
A.5.1.1 Policies for information security	All XX-1 controls
A.5.1.2 Review of the policies for information security	All XX-1 controls
A.6 Organization of information security	
A.6.1 Internal organization	
A.6.1.1 Information security roles and responsibilities	All XX-1 controls, CM-9, CP-2, PS-7, PS-9, SA-3, SA-9, PM-2, PM-10
A.6.1.2 Segregation of duties	AC-5
A.6.1.3 Contact with authorities	IR-6
A.6.1.4 Contact with special interest groups	SI-5, PM-15
A.6.1.5 Information security in project management	SA-3, SA-9, SA-15
A.6.2 Mobile devices and teleworking	
A.6.2.1 Mobile device policy	AC-17, AC-18, AC-19
A.6.2.2 Teleworking	AC-3, AC-17, PE-17
A.7 Human Resources Security	
A.7.1 Prior to Employment	
A.7.1.1 Screening	PS-3, SA-21
A.7.1.2 Terms and conditions of employment	PL-4, PS-6
A.7.2 During employment	
A.7.2.1 Management responsibilities	PL-4, PS-6, PS-7, SA-9
A.7.2.2 Information security awareness, education, and training	AT-2, AT-3, CP-3, IR-2, PM-13
A.7.2.3 Disciplinary process	PS-8
A.7.3 Termination and change of employment	

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS
A.7.3.1 Termination or change of employment responsibilities	PS-4, PS-5
A.8 Asset Management	
A.8.1 Responsibility for assets	
A.8.1.1 Inventory of assets	CM-8
A.8.1.2 Ownership of assets	CM-8
A.8.1.3 Acceptable use of assets	PL-4
A.8.1.4 Return of assets	PS-4, PS-5
A.8.2 Information Classification	
A.8.2.1 Classification of information	RA-2
A.8.2.2 Labelling of Information	MP-3, PE-22
A.8.2.3 Handling of Assets	MP-2, MP-4, MP-5, MP-6, MP-7, PE-16, PE-18, PE- 20, SC-8, SC-28
A.8.3 Media Handling	
A.8.3.1 Management of removable media	MP-2, MP-4, MP-5, MP-6, MP-7
A.8.3.2 Disposal of media	MP-6
A.8.3.3 Physical media transfer	MP-5
A.9 Access Control	
A.9.1 Business requirement of access control	
A.9.1.1 Access control policy	AC-1
A.9.1.2 Access to networks and network services	AC-3, AC-6
A.9.2 User access management	
A.9.2.1 User registration and de-registration	AC-2, IA-2, IA-4, IA-5, IA-8
A.9.2.2 User access provisioning	AC-2
A.9.2.3 Management of privileged access rights	AC-2, AC-3, AC-6, CM-5
A.9.2.4 Management of secret authentication information of users	IA-5
A.9.2.5 Review of user access rights	AC-2
A.9.2.6 Removal or adjustment of access rights	AC-2
A.9.3 User responsibilities	
A.9.3.1 Use of secret authentication information	IA-5
A.9.4 System and application access control	
A.9.4.1 Information access restriction	AC-3, AC-24
A.9.4.2 Secure logon procedures	AC-7, AC-8, AC-9, IA-6
A.9.4.3 Password management system	IA-5
A.9.4.4 Use of privileged utility programs	AC-3, AC-6
A.9.4.5 Access control to program source code	AC-3, AC-6, CM-5
A.10 Cryptography	
A.10.1 Cryptographic controls	
A.10.1.1 Policy on the use of cryptographic controls	SC-13
A.10.1.2 Key Management	SC-12, SC-17
A.11 Physical and environmental security	
A.11.1 Secure areas	
A.11.1.1 Physical security perimeter	PE-3*
A.11.1.2 Physical entry controls	PE-2, PE-3, PE-4, PE-5

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS
A.11.1.3 Securing offices, rooms and facilities	PE-3, PE-5
A.11.1.4 Protecting against external and environmental threats	CP-6, CP-7, PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23
A.11.1.5 Working in secure areas	AC-19(4), SC-42*
A.11.1.6 Delivery and loading areas	PE-16
A.11.2 Equipment	
A.11.2.1 Equipment siting and protection	PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23
A.11.2.2 Supporting utilities	CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PE-15
A.11.2.3 Cabling security	PE-4, PE-9
A.11.2.4 Equipment maintenance	MA-2, MA-6
A.11.2.5 Removal of assets	MA-2, MP-5, PE-16
A.11.2.6 Security of equipment and assets off-premises	AC-19, AC-20, MP-5, PE-17
A.11.2.7 Secure disposal or reuse of equipment	MP-6
A.11.2.8 Unattended user equipment	AC-11
A.11.2.9 Clear desk and clear screen policy	AC-11, MP-2, MP-4
A.12 Operations security	
A.12.1 Operational procedures and responsibilities	
A.12.1.1 Documented operating procedures	All XX-1 controls, SA-5
A.12.1.2 Change management	CM-3, CM-5, SA-10
A.12.1.3 Capacity management	AU-4, CP-2(2), SC-5(2)
A.12.1.4 Separation of development, testing, and operational environments	CM-4(1), CM-5*
A.12.2 Protection from malware	
A.12.2.1 Controls against malware	AT-2, SI-3
A.12.3 Backup	
A.12.3.1 Information backup	CP-9
A.12.4 Logging and monitoring	
A.12.4.1 Event logging	AU-3, AU-6, AU-11, AU-12, AU-14
A.12.4.2 Protection of log information	AU-9
A.12.4.3 Administrator and operator logs	AU-9, AU-12
A.12.4.4 Clock synchronization	AU-8
A.12.5 Control of operational software	
A.12.5.1 Installation of software on operational systems	CM-5, CM-7(4), CM-7(5), CM-11
A.12.6 Technical vulnerability management	
A.12.6.1 Management of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5
A.12.6.2 Restrictions on software installation	CM-11
A.12.7 Information systems audit considerations	
A.12.7.1 Information systems audit controls	AU-5*
A.13 Communications security	
A.13.1 Network security management	
A.13.1.1 Network controls	AC-3, AC-17, AC-18, AC-20, SC-7, SC-8, SC-10
A.13.1.2 Security of network services	CA-3, SA-9
A.13.1.3 Segregation in networks	AC-4, SC-7
A.13.2 Information transfer	

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS
A.13.2.1 Information transfer policies and procedures	AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, PE-17, SC-7, SC-8, SC-15
A.13.2.2 Agreements on information transfer	CA-3, PS-6, SA-9
A.13.2.3 Electronic messaging	SC-8
A.13.2.4 Confidentiality or nondisclosure agreements	PS-6
A.14 System acquisition, development, and maintenance	
A.14.1 Security requirements of information systems	
A.14.1.1 Information security requirements analysis and specification	PL-2, PL-7, PL-8, SA-3, SA-4
A.14.1.2 Securing application services on public networks	AC-3, AC-4, AC-17, SC-8, SC-13
A.14.1.3 Protecting application services transactions	AC-3, AC-4, SC-7, SC-8, SC-13
A.14.2 Security in development and support processes	
A.14.2.1 Secure development policy	SA-3, SA-15, SA-17
A.14.2.2 System change control procedures	CM-3, SA-10, SI-2
A.14.2.3 Technical review of applications after operating platform changes	CM-3, CM-4, SI-2
A.14.2.4 Restrictions on changes to software packages	CM-3, SA-10
A.14.2.5 Secure system engineering principles	SA-8
A.14.2.6 Secure development environment	SA-3*
A.14.2.7 Outsourced development	SA-4, SA-10, SA-11, SA-15, SR-2, SR-4
A.14.2.8 System security testing	CA-2, SA-11
A.14.2.9 System acceptance testing	SA-4, SR-5(2)
A.14.3 Test data	
A.14.3.1 Protection of test data	SA-15(9)*
A.15 Supplier Relationships	
A.15.1 Information security in supplier relationships	
A.15.1.1 Information security policy for supplier relationships	SR-1
A.15.1.2 Address security within supplier agreements	SA-4, SR-3
A.15.1.3 Information and communication technology supply chain	SR-3, SR-5
A.15.2 Supplier service delivery management	
A.15.2.1 Monitoring and review of supplier services	SA-9, SR-6
A.15.2.2 Managing changes to supplier services	RA-9, SA-9, SR-7
A.16 Information security incident management	
A.16.1 Managing of information security incidents and improvements	
A.16.1.1 Responsibilities and procedures	IR-8
A.16.1.2 Reporting information security events	AU-6, IR-6
A.16.1.3 Reporting information security weaknesses	SI-2
A.16.1.4 Assessment of and decision on information security events	AU-6, IR-4
A.16.1.5 Response to information security incidents	IR-4
A.16.1.6 Learning from information security incidents	IR-4

ISO/IEC 27001 REQUIREMENTS AND CONTROLS	NIST SP 800-53 CONTROLS
A.16.1.7 Collection of evidence	AU-4, AU-9, AU-10(3), AU-11*
A.17 Information security aspects of business continuity management	
A.17.1 Information security continuity	
A.17.1.1 Planning information security continuity	CP-2
A.17.1.2 Implementing information security continuity	CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13
A.17.1.3 Verify, review, and evaluate information security continuity	CP-4
A.17.2 Redundancies	
A.17.2.1 Availability of information processing facilities	CP-2,CP-6, CP-7
A.18 Compliance	
A.18.1 Compliance with legal and contractual requirements	
A.18.1.1 Identification of applicable legislation and contractual requirements	All XX-1 controls
A.18.1.2 Intellectual property rights	CM-10
A.18.1.3 Protection of records	AC-3, AC-23, AU-9, AU-10, CP-9, SC-8, SC-8(1), SC-13, SC-28, SC-28(1)
A.18.1.4 Privacy and protection of personal information	Appendix J Privacy controls
A.18.1.5 Regulation of cryptographic controls	IA-7, SC-12, SC-13, SC-17
A.18.2 **Information security reviews**	
A.18.2.1 Independent review of information security	CA-2(1), SA-11(3)
A.18.2.2 Compliance with security policies and standards	All XX-1 controls, CA-2
A.18.2.3 Technical compliance review	CA-2

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

*** End of Document ***