SPJ GLOBAL S P Jain School of Global Management DUBAI • MUMBAI • SINGAPORE • SYDNEY	**Information and Cyber Security Policy**
Document Type	Policy
Administering Entity	Chief Information Security Officer (CISO), Director (Head) – Information Technology (IT), Director – People and Culture, IT Department Staff, Vice President Administration, Department Heads
Latest Approval/ Amendment Date	10 December, 2025
Last Approval/ Amendment Date	New Policy
Approval Authority	Board of Directors
Indicative time of Review	9 December, 2027

1. Purpose

a. The purpose of the policy is to ensure the effective protection and proper usage of the information and communication systems of S P Jain School of Global Management (S P Jain / the School). The Policy aims to protect S P Jain's operations from avoidable damage or harm arising from information and Cyber-security related risks by:

i. Defining agreed information security principles within the organisation;

ii. Defining the roles and responsibilities of S P Jain employees;

iii. Providing a framework for implementing information security management in S P Jain;

iv. Raising awareness of security risks relating to information and IT infrastructure used by S P Jain, and

v. Fulfilling S P Jain's audit and legal obligations.

b. The *Information and Cyber Security Policy* provides the framework for the development, approval, publication and periodic review of security policies, procedures and standards for S P Jain. The policy is supported by standards and procedures approved by Chief Information Security Officer (CISO) and Head - IT that provide guidance for action to achieve the objectives of the policy. It provides a detailed set of actions/steps that sets out the standard and required practice for implementation of a policy with technology specific requirements and implementation process for complying with the policies along with the defined roles and responsibilities.

2. Scope

a. This policy applies to:

i. all information assets, data, and systems under the control or custody of S P Jain;

ii. all IT infrastructure, including applications, databases, networks, and devices;

iii. all personnel including employees, faculty, students, contractors, third-party service providers, and visitors with system or information access (all collectively referred to as 'users');

iv. all modes of access, including on-campus, remote, mobile and cloud-based environments, and covers all activities involving the creation, transmission, storage, or processing of institutional information, and

v. all campuses, data centres, and digital platforms operated or managed by S P Jain.

b. The Policy also applies to any external entities, vendors or partners who process, manage, or store information on behalf of S P Jain, whether through contractual or operational arrangements.

3. Definitions

a. **Information Assets:** All forms of data, information and supporting infrastructure including hardware, software, network resources, cloud services and personnel, that enable S P Jain's operations, teaching, research and decision-making.

b. **Cybersecurity:** The protection of internet-connected systems — including hardware, software and data, against cyber threats such as unauthorised access, attacks, damage or disruption.

c. **Information Security Incident:** Any event that actually or potentially compromises the confidentiality, integrity or availability of S P Jain's information, systems or services.

d. **CISO:** Chief Information Security Officer, responsible for managing S P Jain information security and cybersecurity program.

e. **Information Security Committee (ISC)**: The governing body responsible for oversight, review, and enforcement of this policy.

4. Guiding Principles

a. Information Security and Cybersecurity are shared responsibilities of all individuals who access or manage S P Jain's information systems and resources.

b. Information Security and Cybersecurity measures shall align with recognised standards, regulatory requirements and the S P Jain's legal obligations.

c. Access to all information and systems shall be properly authorised, securely authenticated and continuously monitored.

d. Security controls shall be implemented to safeguard the confidentiality, integrity and availability of information and systems.

e. S P Jain shall undertake continuous review and improvement of its Information Security and Cybersecurity practices to ensure they remain effective and relevant.

5. Information Security Management Framework

a. **Third Party and Outsourcing:** Access to S P Jain's processing facilities and IT System are restricted and controlled for third party service providers, outsourced entities and contractors. Controls implemented following a structured risk assessment process include physical and logical access restrictions, management approvals, and incorporation of relevant information-security clauses in all third-party and outsourcing contracts.

b. **Asset Management:** S P Jain is responsible for protecting its information assets from unauthorised access, modification, disclosure, transmission or destruction. Asset handling and asset labelling procedures shall be developed in order to ensure the security, reliability, integrity, and availability of information.

c. **Human Resource Security:** All employees, contractors and third-party users will be appropriately screened prior to engagement to reduce risks associated with human error, theft, fraud or misuse of S P Jain's resources. Roles and responsibilities, as well as terms and conditions of employment or engagement, are clearly defined in confidentiality and service agreements. All users will receive induction and periodic training on S P Jain's information security policies and procedures.

d. **Acceptable Usage:** S P Jain's information assets and IT resources are provided strictly for authorised academic and business purposes. Users must adhere to safe and responsible usage practices that do not hinder operations, damage S P Jain's reputation or create legal or regulatory exposure. Refer to the *Information Technology Policy* for requirements.

e. **Anti-Virus**: All IT systems of S P Jain must be protected against malicious code through approved enterprise-level antivirus solutions. The antivirus suite shall ensure early detection, efficient containment and prompt removal of malicious code. All systems must have up-to-date antivirus software installed to safeguard against existing and emerging malware threats. Refer to the *Information Technology Policy* for requirements.

f. **Incident Management**: All actual or attempted security breaches, as well as any discovered security weaknesses, must be reported immediately. The incident management process shall ensure that every reported event is promptly investigated, contained and remediated, with corrective actions implemented to prevent recurrence.

g. **Physical and Environmental Security**: All facilities housing S P Jain’s critical IT assets must be adequately protected against unauthorised physical access, damage or environmental hazards. Physical access and the movement of assets shall be continuously monitored, logged and reviewed. Refer to the *Records Management Policy* for more details.

h. **Operations and Security Management**: Appropriate systems and procedures will be implemented periodically to ensure the security, stability and integrity of all IT operations. Operating systems and platforms must be kept current with vendor-released security patches. Regular monitoring shall be conducted, periodic backups must be performed in line with legal, regulatory and institutional requirements. Data shall be purged at periodic intervals depending on the Contractual, Legal and Regulatory requirements.

i. **Information and Communication Management:** S P Jain’s enterprise email system shall be configured and managed to ensure high availability, optimal performance and protection from threats such as malware, unauthorised access and spam. Access to external websites shall be controlled to reduce exposure to malicious content, and access to sensitive data shall be restricted in accordance with privacy and data protection requirements.

j. **Access Control**: User access is granted strictly based on approved business requirements and appropriate authorisation. Access to sensitive information and systems is protected by strong authentication mechanisms (e.g., passwords or access codes) that remain secure throughout their lifecycle — including generation, transmission, storage and use.

k. **Network Security:** S P Jain’s network infrastructure shall be securely designed, implemented and managed to ensure the protection of information transmitted across the network and supporting infrastructure. All remote access will be authenticated and granted only based on legitimate business requirements. The network will be maintained for high availability and periodically tested for vulnerabilities, which must be remediated promptly.

l. **Disaster Recovery and Business Continuity:** All information systems critical to the S P Jain’s operations must have appropriate continuity measures to ensure uninterrupted functionality in the event of disasters or significant disruptions. A Disaster Recovery Plan shall be developed, maintained and tested in accordance with S P Jain’s *Business Continuity Plan (BCP).*

m. **Compliance:** All employees, contractors and third parties must comply with applicable laws, statutory and regulatory directives, contractual obligations, and S P Jain’s internal policies, procedures and guidelines related to Information Security and Cybersecurity.

6. External Regulation/Legislation

a. This Policy aligns with applicable global, national and regional legislation and regulatory requirements governing Information Security, Cybersecurity and Data Protection in the jurisdictions where S P Jain operates. This includes the Privacy Act 1988 (Cth), Australian Privacy Principles (APPs), Security of Critical Infrastructure Act 2018 (SOCI Act) for Sydney, Personal Data Protection Act 2012 (PDPA) and Cybersecurity Act 2018 for Singapore, Federal Decree-Law No. 45 of 2021 (PDPL) and Dubai Electronic Security Center (DESC) Information Security Regulation (ISR) for Dubai, Digital Personal Data Protection (DPDP) Act, 2023, Information Technology Act, 2000 (IT Act) and CERT-In Directions (2022) for India.

b. This policy also ensures compliance with contractual obligations, accreditation requirements and standards prescribed by regulatory or funding authorities relevant to S P Jain's operations.

7. Roles and Responsibilities

a. Managers / Department Heads along with the respective department staff under the specific function and areas are responsible for implementing the policy, as outlined below:

i. The Head – Information Technology (IT) / CISO and staff in IT Department for driving the entire Information Security efforts

ii. The Head - IT and staff in the IT Department are responsible for implementing the policy for IT related areas.

iii. The legal counsel for formulating the Non-Disclosure Agreements (NDAs) and where needed seeking external consultation post approval from the President.

iv. The Vice President – Administration and designated staff in the various administrative departments are responsible for implementing the policy for the physical security, administration and facilities related areas.

v. The Director – People and Culture and staff in the People and Culture Department are responsible for implementing the policy for the Human Resource security related areas.

b. Staff, students, visitors and contractors are required to follow guidelines for safe use of S P Jain's IT resources.

8. Training / Implementation

a. To ensure effective implementation of this Policy, S P Jain promotes a culture of awareness and accountability through structured awareness programs. All personnel who access or manage information systems must be familiar with S P Jain's Information Security and Cybersecurity requirements.

b. The IT Department, under the guidance of the Head – IT / Director – IT / CISO, will design and conduct periodic training and awareness programs covering key aspects of Information Security, Cybersecurity, acceptable use, data protection and incident reporting procedures.

c. Participation in these programs is mandatory for all employees, faculty members, contractors, and relevant third-party service providers who have access to S P Jain’s systems, data, or infrastructure.

d. Specialised or role-based training will be provided to individuals handling sensitive information or performing security-critical functions.

e. The content and format of training programs shall be reviewed and updated regularly to reflect emerging threats, changes in technology, revisions to this Policy, and lessons learned from security incidents.

f. Records of attendance and completion shall be maintained by the IT Department as part of S P Jain’s compliance and audit process.

9. Control and Monitoring

a. S P Jain will implement layered control mechanisms to ensure ongoing protection of information assets and continuous monitoring of system integrity, access, and performance.

b. Security controls shall be preventive, detective, and corrective in nature to provide a balanced and proactive approach to risk management.

c. Continuous monitoring tools and audit trails shall be employed to identify unauthorised access, data leakage, configuration changes, or anomalous activity across systems, applications, and networks.

d. The IT Department, under the direction of the CISO, shall:

i. review and update monitoring controls at least annually or when material changes occur in the technology landscape;
ii. ensure real-time alerting and escalation procedures;
iii. conduct vulnerability assessments and penetration testing at defined intervals; and
iv. ensure remediation of identified risks and weaknesses within approved timeframes.

e. All critical logs (including authentication, system access, and privileged account activities) shall be retained securely for audit and investigation purposes, in accordance with the *Records Management Policy.*

f. Internal and external audits shall be conducted periodically to verify compliance with this policy, supporting standards, and applicable regulations.

g. The Information Security Committee (ISC) shall review audit findings, direct corrective or disciplinary actions where necessary, and oversee continuous improvement initiatives.

h. Audit results and key performance indicators shall be reported to senior management and the Board as part of S P Jain’s overall governance and assurance mechanisms.

10. Breaches and Penalties

a. Violation or any attempted violation of the Information and Cybersecurity Policy shall result in disciplinary action.

11. Exceptions

a. Exceptions to this Policy shall not be universal. In rare circumstances exceptions may arise due to local circumstances, technical constraints or legal obligations existing at a given time.

b. Such exceptions may be approved by CISO on a case-by-case basis, following an official written request by the relevant Information Owner.

Related Documents

a. Information Technology Policy
b. Records Management Policy
c. Privacy Policy
d. Terms of Reference of the Information Security Committee (ISC)
e. Business Continuity Plan

Policy History and Updates Approved by the BOD

Version	Date Executed	Revisions	Approval
1	10 December 2025	New Policy	Board of Directors