Information Security Policy
Indian Institute of Science

1. Objective

As India's premier research institute, it is crucial for IISc (Indian Institute of Science) to protect the Confidentiality, Integrity and Availability of its' information assets. The objective of this Information Security Policy is to outline the necessary measures to safeguard the Institution's information assets from threats, whether internal or external, deliberate or accidental.

2. Supporting Policies

This policy supports and should be read in conjunction with the below:

1. Acceptable Use Policy
2. Minimum security baseline standards
3. Cyber Crisis Management Plan (Under preparation)

3. Scope

This policy applies to all faculty, staff, contractors, students, researchers, interns and any other individuals who have access to the Institution's information resources. It covers all information, regardless of the medium (electronic, paper, or others), and all systems that store, process, or transmit this information.

This policy will be distributed to all new and current faculty, staff, contractors, students, researchers, interns and any other individuals who have access to the Institution's information resources. The policy will also be published on the Institute's website. All users are expected to familiarise themselves with this policy and adhere to its guidelines.

4. Definitions

1. **Information asset:** Any data, information, or system that holds value and is critical to supporting the institution's educational, research, administrative, and operational activities.
2. **Confidentiality:** Ensuring that information is accessible only by those authorised to have access.

3. **Integrity:** Ensuring the accuracy, completeness and consistency of information and safeguarding it from unauthorised modification.
4. **Availability:** Ensuring that information and resources are accessible to authorised users whenever needed.

5. Roles and Responsibilities

- **Director** - The Director of the Institute will be responsible to review and approve the Information Security Policy.
- **Chief Information Security Officer** – The CISO (Chief Information Security Officer) will be the authority and be responsible for the development, implementation, and enforcement of the Information Security Policy. The CISO will explore opportunities and imperatives for continuous improvements and updates to the Policy. The CISO will also drive the cyber security strategy for the Institute, lead security awareness and training initiatives. The CISO will bring to the notice of Information Security Steering Committee any information security concerns that would need the attention of the senior management of the Institute.
- **DIGITS** – DIGITS (Digital Campus and IT Services) team will be responsible for managing and securing the Institution's IT infrastructure, including servers, networks, applications, desktops, laptops and other end user devices. DIGITS will also implement technical controls as per this policy.
- **Information Security Governance Board** – The Director shall establish and Chair an Information Security Governance Board for the Institute, with the responsibility to provide oversight to the implementation of the Information Security Policy and associated information security programmes. The Board will comprise of the Dean (Administration & Finance), Dean (Planning & Infrastructure), the Registrar, Chair - DIGITS, with CISO serving as the convenor. The Board will convene at least once a year.
- **Information Security Steering Committee** – The Director shall constitute an Information Security Steering Committee of the Institute with the responsibility to support the implementation of the Information Security Policy and associated programmes, review and resolve any concerns raised by anyone in the Institute regarding the Policy objectives, expectations and implementation. Dean, Finance and Administration will be the Chairperson of the Information Security Steering Committee. The Committee will also include Deans of Faculties (including UG), Deans of Divisions, Chair – DIGITS, with the CISO as the Convenor.
- **Chairs of the Departments** – The respective Chairs of the Departments at the Institute will be the authority and be responsible for enforcing the policy within the Department, and be the SPOC (Single Point of Contact) for the CISO for any information security concerns.
- **Data Owners** - Individuals or departments that have administrative control over specific types of data will be considered as the owners of the data. They are responsible for ensuring the data is classified appropriately and protected according to its classification

level. The Data Owners will also be responsible for owning and addressing the vulnerabilities identified in the information assets.

- **System Administrators –** Individuals who are in charge of and responsible for managing the IT systems which provide the service will be considered as the System Administrator. For centrally managed IT systems, the System Administrator will be from the DIGITS team, and will work in collaboration with the Data Owner to align and prioritise their requirements for existing and new information systems with the ongoing management of the existing IT facilities and services. For IT systems that are managed within a Department, the Data Owner will nominate the System Administrator for such systems. The System Administrators must manage these systems to the minimum-security baseline as defined by the CISO.
- **Users** - All individuals who access the Institution's information systems are responsible for complying with this policy, protecting the information they handle, and reporting any security incidents.

6. Information Classification

All information in the Institute must be classified based on its sensitivity and value. The classification levels are as follows:

- **Sensitive:** Any information that contains one or more of the following will be deemed Sensitive.
  - All Personally Identifiable Information
  - Government issued identity details like Aadhaar, PAN, Driver's License, Passport, etc
  - Financial information like bank account number, income tax details, etc
  - Health information like medical records, disability status, etc
  - Biometric information like fingerprints, iris scans, facial data, DNA information, etc
  - Sensitive personal data like passwords
  - Sensitive unpublished research related data

  All information classified as Sensitive must be handled with extreme caution. Sharing this information with external parties, except when legally required, should only be done after securing a clear non-disclosure agreement that ensures due care in handling the data.

  Any breach of such information would have serious consequences including risk to the privacy of the individual(s), reputational damage, financial / commercial impact, regulatory risks, etc and hence should be immediately reported to the CISO, who will in turn decide on reporting the breach to other internal and external agencies as necessary.

- **Confidential:** Information that is not classified as Sensitive but is not intended to be shared widely either within or outside the Institute must be classified as Confidential. Examples of Confidential information include

- Personnel information that are not deemed Sensitive
- Educational records

Sharing of Confidential information with external parties, except when legally required, should only be done after securing a clear non-disclosure agreement that ensures due care in handling the data.

Any breach of such information would have serious consequences including risk to the privacy of the individual(s), reputational damage, financial / commercial impact, regulatory risks, etc and hence should be immediately reported to the CISO, who will in turn decide on reporting the breach to other internal and external agencies as necessary.

- **Internal:** Information that is not classified as Sensitive or Confidential but is not intended to be shared outside the Institute must be classified as Internal. Examples of Internal information would include
  - Academic information like grading rubrics, teaching data, attendance records, etc
  - Administrative information like internal memos, minutes of meetings, internal emails, etc
  - Unpublished research information
  - IT and infrastructure information like architecture diagrams, system specifications, incident logs, etc
  - Information shared on campus bulletin, internal newsletters, etc

- **Public:** Information that can be freely shared with public without any negative impact on the Institution. This could include faculty profiles, published research papers, etc.

7. Information Security Awareness

All faculty, staff, contractors, students, researchers, interns and any other individuals who have access to the Institution’s information resources must undergo the Information Security awareness training as decided by the CISO, including periodic mandatory refresher trainings.

8. Data privacy

Privacy and protection of personal information shall be ensured as required in relevant legislation and regulation where applicable.

9. Acceptable Use

The Institute's Acceptable Use Policy defines the expected behaviors that all users of IT facilities and services must comply with. It specifies guidelines for the acceptable and prohibited use of the Institute's IT resources.

10. IT Asset Management

1. Data Owners must know what data, IT systems, software, cloud services and storage they use.
2. The CISO team will create and manage a Central IT Asset Register for the Institute.
3. Data Owners – or their delegates – must maintain and update the Institute's designated Central IT Asset Register on an ongoing basis.

11. Secure System Implementation

When planning or developing new information systems, Data Owners or their nominated System Administrators must perform an information security risk assessment. DIGITS must also conduct a security review before the system goes live. Data Owners should notify DIGITS as early as possible to:

1. Identify any security risks related to the changes.
2. Ensure the system meets security and design standards.
3. Use the Institute's resources efficiently.
4. Evaluate the system's impact on existing systems.

12. Access Management

1. All users must be authenticated before accessing any information systems.
2. Multi-factor authentication (MFA) is required for accessing sensitive or critical systems, including emails, VPN and other systems as deemed necessary by the CISO.
3. Access to information should be granted based on the principle of least privilege. Users are given the minimum level of access necessary to perform their duties.
4. User accounts must be managed, and access reviewed regularly. Inactive accounts should be disabled and removed after a defined period.

13. Data protection

1. Sensitive data must be encrypted in transit and at rest using strong encryption algorithms.
2. Regular backups must be performed for critical data. Backups must be encrypted and stored in a secure location.
3. Data must be retained according to the Institution's data retention policy and securely disposed of when no longer needed.

14. Network security

1. Firewalls must be implemented to protect the Institution's network from unauthorised access and external threats.
2. Critical systems and sensitive information should be isolated from less secure network segments through appropriate network segmentation.
3. Network traffic must be monitored continuously for suspicious activities, and intrusion detection/prevention systems (IDS/IPS) must be employed.

15. Information Security Incident Management

1. Information Security incidents and abnormal behaviour associated with information and / or systems need to be reported and responded appropriately to minimise their damage.
2. Any suspected information security incident must be reported to the CISO by email to ciso@iisc.ac.in.
3. All incidents must be logged, and the logs should be reviewed periodically to identify patterns or trends that could indicate a broader issue.
4. If there is a suspected or confirmed information security breach, CISO team may, with or without consulting the relevant Data Owner or System Administrator, require that any systems believed to be compromised are made inaccessible.
5. Incident Response plans must be developed and maintained for common incidents. This plan should outline the steps for identifying, containing, eradicating, and recovering from security incidents.

16. Third Party Risk Management

Each contract with a third party will identify the obligation that the third party maintains the security of the organisation's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

17. Physical and Environmental Security

1. Institute's processing facilities that contain Sensitive or Confidential information must be physically protected from unauthorised access, damage and interference.
2. Organisation's Information Assets must be sited in secure areas, protected by a defined security perimeter, with appropriate entry controls and security mechanisms.
3. Data Centres and server rooms must be equipped with environmental controls, such as fire suppression systems, temperature control and UPS (Uninterruptible Power Supplies).
4. Portable devices like laptops should be securely stored whenever they are not being used.
5. Lock computer workstations when the workspace is unattended.
6. Secure all sensitive or confidential hardcopy information in the workspace when it will be left unattended for an extended time.
7. Report any theft or loss of Institute's IT Assets to the CISO as soon as you become aware of it.

18. Exceptions management

1. Exceptions to the Information Security Policy shall be allowed based on a specific or peculiar manifestation of circumstances which could be temporary in nature.
2. Any exception to this Policy shall be approved by the CISO. The CISO could in turn escalate the approval to the Information Security Steering Committee or the Director for cases that are deemed needing their attention.
3. All exceptions will be time-bound and not permanent in nature.
4. Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the requestor.

19. Clarifications

Please write to ciso@iisc.ac.in for any clarification related to the Information Security Policy with respect to its interpretation, applicability and implementation.

Information Security Policy
Indian Institute of Science

Signatures:

Joy kuri

Chief Information Security Officer

Submitted for Approval

Recommended for approval

Recommended for Approval

G. Rangarajan

Director

Approved