IT SECURITY POLICY

(Policy #ITKM03 IT Security Policy V1.1)

RELEASE CONTROL

Version No:	Details
V 0.2	Pre-release, the purpose of prerelease is to inform all stake holders about the issuance of this policy and also to give advance intimation to the assured departments to get prepared.
V 1.0	First release

POLICY OWNER

Department:	Represented by:
Registrar	Dr. S. Ponnusamy

POLICY RATIFIED BY:

IT Policy and Process Reengineering Committee members.

POLICY ASSURED BY:

Department	Represented by	Applicable to
Directors / Deans / HODs	Individual Role Holders	Respective users using computing assets.

TABLE OF CONTENTS

1. OBJECTIVE

The purpose of this IT security policy is to protect the digital information assets of SRMIST from all threats, internal, external, deliberate or accidental. The policy is aimed at the Institution,

- Safeguarding the availability, confidentiality and integrity of the University's information.
- Protecting the IT assets and services of the University against unauthorised access, intrusion, disruption or other damage.
- Ensuring compliance with applicable legislation and regulations.
- Providing governance with clear responsibility and accountability.

2. SCOPE

This policy applies to everyone (including, but not limited to, all SRMIST faculty, staff, students, visitors, vendors, contractors, and employees of an affiliated entity) who accesses Data or University networks or who stores Data through the use of SRMIST credentials or under the authority of and pursuant to University contracts.

- This policy also applies to such access and storage by SRMIST Community Members whether the Data is accessed, stored or otherwise resides on University owned or controlled devices, personally owned or controlled devices, or devices owned or controlled by a third party under contract with the SRMIST.

2.1. YOUR RIGHTS AND RESPONSIBILITIES

a) SRMIST has a responsibility for safe guarding the confidentiality of information through the protection of information from unauthorized disclosure with access only by entitlement.

b) All users, students and staff are required to demonstrate compliance to Security Policy, in order to protect the confidentiality, integrity, and availability of SRMIST's IT Assets. This policy also extends to contractors, consultants and/or 3rd parties providing services to SRMIST.

c) Centralized IT Services (ITKM) is responsible for administering the information security functions in the SRMIST network using various IT security tools and appliances.

3. POLICY DETAILS

- The SRMIST expects members of its faculty, staff, and student body to understand and mitigate the IT security risks inherent in digital technologies. SRMIST also requires members of its faculty, staff, and student body to protect the SRMIST's resources that include information assets, software, hardware, and facilities by adhering to the Information Security guidelines.
- All members of SRMIST including consultants, outside vendors and visitors to campus who have access to SRMIST-owned or managed information through computing systems or devices, must maintain the security of that information and those systems and devices.
- Respective directorate should ensure that the Sensitive Information, in all forms – written, electronically recorded, or printed – are protected from accidental or intentional unauthorised modification, destruction, or disclosure. Appropriate access and security controls are to be followed in the transmission and storage of confidential data, and adequate precautions must be taken to ensure that only the intended recipient can access the data.
- Backups are a must for any organisation, especially considering regulatory compliance and the ever-increasing cyber security threats for which businesses are at high risk. The directorate/faculty should ensure that a reliable backup and data recovery strategy is in place to ensure the confidentiality, integrity, and availability of critical data related to academic / research/business processes.
- Departments / Business units will never ask for full details of any member's password or other security credentials (unless the user has self-initiated a password reset with the ITKM Service Desk). Therefore, users should never share their passwords with others.

- Faculty / Directorate to ensure that their respective computing Assets that are connected to SRMIST network have been protected with appropriate licensed anti-virus and anti-malware tools.

3.1. USER AUTHENTICATION AND ACCESS

- Authentication is required for each connection to the network. Single Sign-on through Web Login allows for a safe and secure computing environment with an added layer of protection.
- Access management using groups and role-based provisioning; for application and service providers.
- User must follow best practices to prevent misuse, loss or unauthorized access to systems:
  - Keep passwords confidential
  - Change passwords regularly
  - Never write down passwords
  - Never send both username and passwords via same email or post
  - Change temporary passwords at first logon
- Do not leave your computer unattended without locking your computer or logging off.

3.2. NETWORK SECURITY AND MONITORING

- All IT assets in SRMIST which includes but is not limited to: servers, workstations, and network access devices are subject to ongoing monitoring. The inappropriate use of these systems and/or networks which violates the University's policies or local, state and federal laws, will be investigated as needed. The Registrar may authorise the Directorate of ITKM to conduct such IT security investigations.
- Automated tools will be used to monitor the SRMIST network in real-time for any notification of detected security events and vulnerabilities for following
  - Internet traffic
  - Electronic mail traffic
  - LAN traffic, protocols, and IT inventory
  - System security parameters

- Where feasible, the following files will be checked for signs of security issues and vulnerability exploitation at a frequency determined by risk:
    - Intrusion detection system logs
    - Firewall logs
    - User account logs
    - Network scanning logs
    - System error logs
    - Application logs
    - Data backup and recovery logs
    - Help Desk trouble tickets
- Faculty / Directorate to ensure that their respective departments' Computing Assets that are connected to SRMIST network to have:
    - Anti-virus installed and up-to-date,
    - Operating System patched with latest security updates

3.3. BACKUP AND DATA RECOVERY

- All SRMIST systems, applications and data must be backed up on a technically practicable schedule suitable to the criticality, integrity, and availability requirements defined by the respective data owners/faculty directorate.
- Information owners of business units and faculty directorates must ensure that appropriate backup and system recovery measures are in place for their Business and Academic data.
- In case the backups are stored off-site, appropriate security measures must be taken to protect against unauthorised disclosure or loss. Recovery procedures should be tested on a regular basis.
- Backups of confidential or sensitive information to be encrypted

- Retention period of backups should be proportionate to the criticality, integrity, and availability needs of the data.
- Backup and recovery documentation must be maintained and periodically reviewed

3.4. DATA PROTECTION

- All sensitive information that is transmitted or received by SRMIST computer systems, including mobile devices, must be encrypted when transmitted over wireless or Public Networks, including when transmitted via FTP and electronic mail.
- Sensitive information should be saved in folders with access limited to those individuals authorized to access the information.
- Users must log off or lock their workstations when not in use.
- Respective directorate/faculty is responsible for the processing and storage of the information or data in their respective computing devices for their academic and business purpose. Data protection should meet the regulations and guidelines of both domestic and international bodies.

3.4.1. GDPR – European Union (EU) General Data Protection Regulation

The European Union's General Data Protection Regulation ("GDPR") imposes data privacy and data protection requirements on entities that control or process personal data about people in the 28 member countries of the European Union ("EU") as well as countries located in the European Economic Area ("EEA"). GDPR's requirements apply to entities located outside of the EU who control or process the personal data of anyone who is in the EU, regardless of EU citizenship. The Directorate of International Relations in collaboration with the Office of General Counsel, Data Stewards, and other key stakeholders maintains documentation and guidance for complying with GDPR requirements.

3.4.2. PERSONAL DATA PROTECTION BILL, 2018

Data protection refers to policies and procedures seeking to minimise intrusion into the privacy of an individual caused by the collection and usage of their personal data.

The Rules define the personal information of an individual as any information which may be used to identify them. They hold the organisation (who is using the data) liable for compensating the individual for negligence in maintaining security standards while dealing with the data.

The Bill sets out certain rights of the data principal (Individual) whose data is being processed. These include (i) the right to obtain a summary of their personal data held with the data fiduciary, (ii) the right to seek correction of inaccurate, incomplete, or outdated personal data, (iii) the right to have personal data transferred to any other data fiduciary in certain circumstances, and (iv) the right 'to be forgotten', which allows the data principal to restrict or prevent continuing disclosure of their personal data.

3.5. ADHERENCE WITH CENTRAL, STATE, LOCAL, CYBER AND APPLICABLE INTERNATIONAL LAWS

SRMIST's guidelines related to use of technologies derived from this concern, including laws regarding license, copyright and the protection of intellectual property. As a user of IT resources of SRMIST, you must:

- Abide by all Central, State, Local, Cyber and applicable international Laws.
- Abide by all applicable Copyright, Data Protection and Privacy Laws.

3.6. ENFORCEMENT

Non-compliance with security policy and guidelines can bring about significant risk and liability for SRMIST, which puts the institution at significant risk of legal action, substantial penalty and substantial damage to the brand name.

Violation of this Policy may result in suspension or loss of the violator's use privileges with respect to Institutional Data and University-owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with SRMIST. Civil, criminal and equitable remedies may apply.

Registrar SRMIST reserves the right to direct ITKM to inspect a faculty or staff member's computer system for violations of this policy. Periodic, random audits shall also be conducted as appropriate and as advised by ITKM.

3.7. USER COMPLIANCE

SRMIST's Conditions to follow the IT security policy. Failure to comply with these could constitute a disciplinary offence. The Registrar SRMIST reserves the right to authorise IT support team to audit without notice to enable them to check against

- Any unlicensed software or hardware or illicit copies of documentation
- Suspect a computer used for official work or study has committed a security breach or is under attack
- Reporting an email spam or phishing attempt
- Reporting unauthorised access and acquisition of computerised data that materially compromises the security or confidentiality of personal information and is reasonably believed to result in loss or injury.
- Reporting a breach of personal data, Under GDPR, Personal Data Breach when it leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any information relating to an identified or identifiable natural person ("personal data") transmitted, stored or otherwise processed by or on behalf of the organisation.