SR UNIVERSITY

IT RESOURCE MANAGEMENT POLICY

The university recognizes the vital role of Information Technology (IT) in supporting its teaching, learning, research, and administrative functions. The University is committed to protecting the confidentiality, integrity, reliability, and availability of its information assets. All users of SRU's IT resources—including faculty, staff, students, researchers, associates, and other authorized individuals—are responsible for using these resources appropriately to support the University's objectives. The IT Policy applies to both University-owned and personally owned devices used to access, store, or transmit University information and establishes guidelines for the secure management and protection of information in all forms.

Scope and objective

IT Policy applies to all individuals who use the University's IT resources, including faculty, staff, administrators, students, guests, and other authorized users, regardless of whether the resources are personally owned or University-owned. Its purpose is to ensure the secure, lawful, and appropriate use of the University's IT infrastructure in support of teaching, learning, research, and administrative activities. The policy establishes responsibilities and controls to protect the confidentiality, integrity, reliability, and availability of information assets, including data, information systems, computers, network devices, intellectual property, documents, and verbal communications.

Definition of Information Technology Resources and Policies

IT Resources include all University-owned, licensed, leased, or contractually managed technology assets and information resources. These comprise electronic and physical information, computer hardware and software, networks, telephone systems, servers, personal computers, wireless infrastructure, and other devices connected to the University's IT environment. The scope also extends to digital resources and services accessible through the internet or intranet, both on and off campus, that are provided by the University for the benefit of its stakeholders.

Protection of IT Information

The Custodian is responsible for protecting sensitive and legally restricted information from unauthorized access, use, or disclosure. Access to such information must be limited to individuals with a legitimate business, academic, or legal need. Any transmission of restricted information outside the University requires proper authorization and must comply with applicable legal and institutional requirements.

Information Policy

The Information Policy defines how sensitive information is identified and protected within the University. It recognizes all organizational data as a valuable asset and requires employees to safeguard confidential information in their possession. The policy applies to information in both physical and electronic formats and establishes appropriate measures to ensure its security and confidentiality.

IT Hardware Installation Policy

Users must ensure proper installation and management of computers and peripherals to minimize service disruptions. Each computer should have a designated responsible user, and departments must assign accountability where multiple users share a system. University-owned computers should be procured with adequate warranty coverage and maintained through annual maintenance contracts after warranty expiration. Any relocation of a computer must be reported to the IT Department to maintain accurate asset and IP address records. Unauthorized changes to registered systems may result in temporary network disconnection until compliance is restored. Users are responsible for regularly backing up important data, while the IT Team is responsible for maintaining and supporting University computer systems.

Software Installation and Licensing Policy

All departments and projects must ensure that computers are procured with properly licensed software, including operating systems, antivirus solutions, and required applications. The installation or use of pirated, unauthorized, or illegal software on university-owned systems or devices connected to the University network is strictly prohibited. Departments or individuals will be held accountable for any violations involving unlicensed software. To ensure standardization, compliance, and efficient management, all IT-related purchases must be coordinated and approved through the University's IT Department.

Database (of e-Governance) Use Policy

University databases and e-Governance systems are valuable institutional assets and must be protected regardless of the sensitivity of the data they contain. Access to data shall be granted based on an individual's role and authorized responsibilities, and information stored in university databases is intended primarily for internal institutional use. Personal and identifiable information must not be disclosed to external parties without proper authorization, and all external requests for information must be routed through the Office of the Registrar. Unauthorized modification, deletion, manipulation, or destruction of data, attempts to compromise database security, or any form of database tampering are strictly prohibited. Violations may result in disciplinary action and, where applicable, legal proceedings in accordance with university regulations and applicable laws.

Policy on Advanced Digital Technologies

The University is committed to the responsible, ethical, and institution-wide adoption of advanced digital technologies, including Artificial Intelligence (AI), the Internet of Things (IoT), data analytics, cloud computing, automation, and smart digital platforms, to enhance institutional governance, academic excellence, operational efficiency, sustainability, and service delivery. The University shall integrate advanced digital technologies into its academic, research, administrative, and campus management functions to support evidence-based decision-making, optimize institutional resources, improve stakeholder services, and strengthen sustainable campus operations. The implementation of these technologies shall align with the University's strategic objectives and promote innovation while ensuring transparency, accountability, fairness, and responsible use.

The University shall utilize AI-enabled analytics, digital dashboards, enterprise resource planning (ERP) systems, smart sensors, Internet of Things (IoT) devices, automation tools, and decision-support systems to facilitate academic administration, student services, research management, infrastructure management, energy and water monitoring, waste management, transportation management, and other sustainability initiatives. These digital systems shall enable real-time monitoring, predictive analysis, resource optimization, and continuous improvement of institutional processes.

All advanced digital technologies deployed by the University shall be periodically evaluated to assess their effectiveness, accuracy, reliability, security, and contribution to institutional performance. User feedback, system performance indicators, internal reviews, and technological advancements shall be considered while upgrading or enhancing digital platforms. The University shall continuously improve its digital ecosystem to ensure operational excellence, resilience, sustainability, and high-quality service delivery across all academic and administrative functions. The Computer Centre, in coordination with the Centre for Software Services and Digital Learning, IQAC, and other concerned departments, shall oversee the implementation, monitoring, periodic evaluation, and continual enhancement of advanced digital technologies across the University.

Data Protection, Privacy and Information Security Policy

SR University recognizes that personal data, institutional information, and digital records are valuable assets requiring appropriate protection throughout their lifecycle. The University is committed to ensuring the confidentiality, integrity, availability, privacy, and lawful processing of all personal and institutional data in accordance with applicable national laws, regulatory requirements, and internationally accepted information security practices.

The University shall comply with the provisions of the Digital Personal Data Protection Act, 2023 (DPDP Act), Government of India, and any other applicable data protection, cybersecurity, and privacy regulations governing the collection, storage, processing, transmission, sharing, retention, and disposal of personal information. For international collaborations, research partnerships, student exchanges, or other activities involving overseas stakeholders, the University shall also take appropriate measures to comply with applicable international data protection requirements, including the principles of the General Data Protection Regulation (GDPR) wherever relevant.

Access to personal and sensitive information shall be governed through role-based authorization, secure authentication mechanisms, and the principle of least privilege. Personal data shall be collected only for legitimate academic, administrative, research, or statutory purposes and shall not be disclosed to unauthorized individuals or organizations except where required by law or with appropriate authorization. The University shall implement appropriate technical and organizational safeguards, including secure network infrastructure, encryption where applicable, authenticated access, firewalls, antivirus protection, regular system updates, secure backups, disaster recovery mechanisms, and continuous monitoring to protect institutional information assets against unauthorized access, alteration, loss, misuse, or cyber threats. Periodic internal audits, vulnerability

assessments, system reviews, and information security evaluations shall be conducted to assess compliance with institutional policies and applicable legal requirements. Findings from such reviews shall be utilized to strengthen cybersecurity controls, improve data governance practices, and enhance the University's digital infrastructure.

The University shall promote awareness of information security and data privacy among faculty, staff, students, researchers, and other stakeholders through institutional policies, user guidelines, training programmes, digital communications, and awareness initiatives. Significant updates to data protection practices shall be communicated transparently to relevant stakeholders. The Computer Centre, in coordination with the Registrar, IQAC, Centre for Software Services and Digital Learning, and other designated authorities, shall be responsible for implementing, monitoring, periodically reviewing, and continuously improving the University's data protection and information security framework.

Open-source and free-to-use software policy

SR University encourages the adoption of Free and Open-Source Software (FOSS) for IT operations wherever it meets institutional requirements. Open-source software may be used without prior approval from the IT Department, subject to the discretion of the respective Dean or authorized authority. Stakeholders are encouraged to prioritize open-source solutions over proprietary alternatives whenever feasible. Proprietary software may be adopted when no suitable open-source option exists. The University also supports making internally developed software available under approved open-source licenses whenever appropriate.

Network Intranet and Internet Use Policy

The University provides secure network access through authenticated connections, including VPN services, and all usage is governed by the IT Policy. The Computer Centre (CC) is responsible for maintaining and supporting the University network, while users must promptly report network-related issues. Access to network resources is granted through authorized user accounts, and account holders are personally responsible for all activities conducted under their credentials. All devices connected to the University network must be registered and assigned an approved IP address by the CC. IP addresses are allocated based on designated network segments and locations, and users may not transfer assigned IP addresses between devices without authorization. Any modifications to network configurations or established protocols require prior approval from the Computer Centre.

E-mail Account Use Policy

The University's email system shall be used primarily for official, academic, administrative, and authorized communications. All faculty, staff, and students are expected to maintain active University email accounts to receive official notifications and announcements. Official communications should be conducted through university-issued email accounts, and personal email accounts should not be used for internal institutional correspondence except under exceptional circumstances with a copy sent to the official account. Users are prohibited from using University email for illegal, commercial, offensive, fraudulent, or unauthorized activities, including spamming and spoofing. Users must exercise caution when handling suspicious emails and attachments, maintain appropriate backups of important communications, and ensure compliance with the University's email usage

requirements. The University retains ownership of official email accounts and their contents, and violations may result in disciplinary action in accordance with university regulations.

Role of IT team

The IT Team and System Administrators are responsible for managing and supporting all IT services and infrastructure at SR University. The System Manager, as Director of the Computer Centre (CC), oversees the implementation of the University's IT Policy. The CC is responsible for maintaining University computer systems, peripherals, websites, and network-related services, as well as resolving hardware, operating system, and authorized software issues. The installation or promotion of unauthorized or illegal software is strictly prohibited. During system maintenance or reinstallation, authorized personnel must preserve network configurations, apply necessary updates and security patches, and ensure antivirus software remains current and effective.

Breach of IT Policy

All users are responsible for remaining vigilant and promptly reporting any suspected or actual IT policy violations, security incidents, or breaches to the System Manager of the Computer Centre or the University Registrar. Any confirmed violation of the IT Policy will be investigated and addressed in accordance with university regulations. The Registrar shall be the designated authority responsible for initiating and overseeing disciplinary or corrective actions related to IT policy violations occurring both within and outside the University campus.