INFORMATION TECHNOLOGY POLICY

2026 Edition

Policy No. : EOMS 21001: 2018/Pol/PHE/2025-2026/03

Sathyabama Institute of Science and Technology

(Deemed to be University)

Rajiv Gandhi Salai, Chennai – 600119, Tamil Nadu, India

TABLE OF CONTENTS

DOCUMENT CONTROL SHEET

Particulars	Details
Policy Title	Information Technology Policy
Policy Number	EOMS 21001: 2018/Pol/PHE/2025-2026/03
Version Number	4.0
Date of Approval	03/07/2026
Reviewed By	IQAC
Approved By	Executive Council
Review Frequency	Once every Three Years
Next Review Due	02/07/2029
Policy Status	Active

DOCUMENT CLASSIFICATION : This document constitutes an official policy of the Deemed to be University. The provisions of this policy shall be implemented and interpreted in accordance with the applicable statutory and regulatory requirements, and in conjunction with other relevant policies, regulations, ordinances, and guidelines of the Institution.

INFORMATION TECHNOLOGY POLICY

1. PREAMBLE

Sathyabama Institute of Science and Technology recognizes Information Technology (IT) as a critical enabler of academic excellence, research innovation, administrative efficiency, governance, and stakeholder engagement. The Institution is committed to providing secure, reliable, accessible, and sustainable information technology infrastructure and services to support teaching, learning, research, consultancy, extension activities, and institutional administration.

This Policy establishes a framework for the effective management, utilization, protection, and governance of Information Technology resources. It seeks to ensure the confidentiality, integrity, availability, and security of information assets while promoting responsible and ethical use of technology by all stakeholders.

The Policy is aligned with applicable statutory requirements, the Information Technology Act, 2000, cyber security best practices, data protection principles, and the Institution's commitment to digital transformation and quality assurance.

2. OBJECTIVES

The objectives of this Policy are to:

- Ensure secure, reliable, and efficient utilization of Information Technology resources.
- Protect the confidentiality, integrity, and availability of institutional information assets.
- Establish governance mechanisms for IT infrastructure and digital services.
- Promote responsible, ethical, and lawful use of technology resources.
- Safeguard institutional data against unauthorized access, misuse, loss, and cyber threats.
- Ensure business continuity through effective backup and disaster recovery mechanisms.
- Facilitate digital transformation in teaching, learning, research, and administration.
- Ensure compliance with applicable laws, regulations, and institutional policies.

3. SCOPE

This Policy applies to all users accessing Information Technology resources of the Institution, including:

- Students
- Faculty Members
- Administrative Staff
- Technical Staff
- Research Scholars
- Consultants
- Contractors
- Temporary Employees
- Guests and Visitors
- External Users authorized by the Institution

The Policy applies irrespective of whether access occurs from within the campus or through remote locations.

4. DEFINITION OF INFORMATION TECHNOLOGY RESOURCES

Information Technology Resources include, but are not limited to:

- Computers, Workstations, and Laptops
- Mobile Devices and Tablets
- Servers and Storage Systems
- Network Infrastructure
- Internet and Wi-Fi Facilities
- Printers, Scanners, and Peripherals
- ERP, LMS, MIS, and Institutional Applications
- Cloud Services and Digital Platforms
- Institutional Websites and Portals
- Electronic Data and Databases
- Licensed Software and Digital Content
- Audio-Visual and Communication Systems

This Policy also applies to personal devices connected to institutional networks and systems.

5. POLICY STATEMENTS

5.1 Acceptable Use of Information Technology Resources

Information Technology resources shall be utilized solely for legitimate academic, research, administrative, and institutional purposes.

Users shall utilize:

- Institutional websites and portals
- Learning Management Systems (LMS)
- Enterprise Resource Planning (ERP) Systems
- Management Information Systems (MIS)
- E-Library Resources
- Collaboration and Communication Platforms
- Research and Academic Computing Resources

All users shall ensure responsible, ethical, and lawful utilization of technology resources.

5.2 Prohibited Activities

The following activities are prohibited:

- Unauthorized access to systems or data.
- Creation or dissemination of offensive, discriminatory, obscene, fraudulent, or unlawful content.
- Activities that compromise network security.
- Circumvention of security controls or network filters.
- Distribution of malicious software.
- Unauthorized software installation.
- Unauthorized commercial use of institutional resources.
- Activities violating applicable laws, regulations, or institutional policies.

Violations may result in disciplinary action.

5.3 Copyright and Software Licensing

The Institution shall ensure compliance with copyright laws and software licensing requirements.

Users shall:

- Respect intellectual property rights.
- Use only authorized software.
- Avoid unauthorized duplication, distribution, or sharing of licensed content.
- Comply with software licensing agreements.

The Institution shall acquire and maintain appropriate academic and enterprise software licenses.

5.4 Social Media and Digital Communication

Users shall exercise responsibility while using social media and digital communication platforms in relation to the Institution.

Institutional information shall not be disseminated through social media or public platforms without authorization from the competent authority.

Users shall:

- Protect institutional reputation.
- Maintain confidentiality of information.
- Follow approved communication protocols.
- Report suspicious digital activities.

5.5 Information Security and Cyber security

The Institution shall implement appropriate information security controls to safeguard digital assets.

Security measures may include:

- Access Control Systems
- User Authentication Mechanisms
- Multi-Factor Authentication
- Firewalls
- Intrusion Prevention Systems
- Endpoint Protection Systems

- Security Monitoring Tools
- Cyber security Awareness Programs

Users shall not attempt unauthorized access to systems, networks, applications, or information resources.

5.6 Unified Threat Management (UTM)

The Institution shall deploy Unified Threat Management (UTM) solutions to ensure secure internet and network access.

UTM mechanisms may include:

- Antivirus Protection
- Anti-Spam Systems
- Web Filtering
- Content Filtering
- Malware Detection
- Threat Prevention Services

Security updates and patches shall be applied periodically.

5.7 Website Governance

The Institution shall maintain official websites and digital platforms to ensure transparency, accessibility, and dissemination of authentic information.

Website governance shall include:

- Content Creation
- Content Review
- Content Approval
- Publishing and Administration
- Security Monitoring

Only authorized and approved content shall be published on institutional websites.

The Institution reserves the right to remove or block content that violates institutional policies or legal requirements.

5.8 Data Backup and Disaster Recovery

The Institution shall establish data backup and disaster recovery mechanisms to ensure business continuity and protection of information assets.

Backup procedures shall include:

- Daily Incremental Backups
- Weekly Backups
- Monthly Full Backups
- Cloud Backup Mechanisms
- Off-site Backup Storage

The Information Technology Department shall periodically test recovery procedures and maintain disaster recovery readiness.

5.9 IT Asset Management

The Institution shall establish procedures for:

- Procurement
- Deployment
- Maintenance

- Utilization
- Inventory Management
- Energy Audit
- Upgrade
- Disposal of Information Technology assets.

All IT assets shall be recorded, monitored, and periodically verified.

5.10 IT Support and Service Management

The Institution shall provide IT support services to ensure uninterrupted academic and administrative operations.

Support services may include:

- Help Desk Services
- Network Support
- Hardware Maintenance
- Software Support
- System Administration
- Emergency Technical Assistance

Appropriate support mechanisms may be available beyond regular working hours for critical requirements.

6. GOVERNANCE FRAMEWORK

The implementation of this Policy shall be overseen by:

- Executive Council
- Vice-Chancellor
- Pro Vice-Chancellor
- Registrar
- Director Administration
- Chief Technical Officer (CTO)
- IT Administrator
- Software Cell
- Website Management Team
- Heads of Schools and Departments

These authorities shall ensure effective implementation, monitoring, review, and continual improvement of Information Technology governance.

7. ROLES AND RESPONSIBILITIES

Chief Technical Officer (CTO)

- Coordinate implementation of the IT Policy.
- Oversee IT governance and infrastructure management.
- Monitor cybersecurity compliance.

IT Administrator

- Manage IT infrastructure and operations.
- Ensure system availability and security.
- Coordinate technical support services.

Software Cell

- Maintain ERP, LMS, MIS, and digital platforms.
- Support users and digital services.

Users

- Comply with this Policy.
- Protect credentials and information assets.
- Report security incidents promptly.

8. COMPLIANCE AND VIOLATION

Any violation of this Policy shall constitute misconduct and may result in disciplinary action in accordance with institutional rules, regulations, and applicable laws.
The Institution reserves the right to monitor, investigate, and take appropriate action regarding misuse of Information Technology resources.

9. MONITORING AND AUDIT

Periodic reviews, audits, vulnerability assessments, and security evaluations shall be conducted to ensure compliance with this Policy and to strengthen the Institution's cyber security posture.

Issued by
Dr.G.Sundari
(Registrar)

Dr. G.SUNDARI, M.E., Ph.D.,
REGISTRAR
SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Jeppiaar Nagar, Rajiv Gandhi Salai,
Chennai-600 119.

S. SRINIVASAN
ADVOCATE-HIGH COURT
&
COMMISSIONER OF OATHS
Chamber No: 13, Law Chambers,
High Court Buildings, Chennai-600 104
Ph: 044-25587404, Cell: 98402 40091

Recommended by
Dr.B.Sheela Rani
(Vice-Chancellor)

Dr.B. SHEELA RANI, M.S. (By Research), Ph.D.,
VICE-CHANCELLOR
SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Jeppiaar Nagar, Rajiv Gandhi Salai,
Chennai - 600 119.