DIGITAL GOVERNANCE AND INFORMATION TECHNOLOGY POLICY

2026 Edition

Policy No. : EOMS 21001: 2018/Pol/DE/2025-2026/01

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	Digital Governance and Information Technology Policy
Policy Number	EOMS 21001: 2018/Pol/DE/2025-2026/01
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.

DIGITAL GOVERNANCE AND INFORMATION TECHNOLOGY POLICY

1. PREAMBLE

Sathyabama Institute of Science and Technology recognizes digital technologies as strategic enablers of academic excellence, research innovation, administrative efficiency, transparency, accountability, and stakeholder engagement. The Institution is committed to leveraging information and communication technologies to strengthen governance, improve service delivery, facilitate data-driven decision-making, and enhance the overall educational experience.

The Institution shall establish a robust digital governance framework to ensure secure, reliable, accessible, and efficient utilization of digital systems and information assets. This Policy provides comprehensive guidelines for e-governance, data protection, privacy management, cyber security, enterprise systems, learning management systems, and digital content governance while ensuring compliance with applicable laws, regulations, and institutional requirements.

2. OBJECTIVES

The objectives of this Policy are to:

1. Promote digital transformation across academic and administrative functions.
2. Strengthen transparency, efficiency, and accountability through e-governance.
3. Ensure protection of institutional data and privacy of stakeholders.
4. Establish cyber security measures to safeguard digital assets.
5. Facilitate effective utilization of ERP and LMS platforms.
6. Promote quality, accessibility, and responsible use of digital content.
7. Support data-driven governance and decision-making.
8. Ensure compliance with statutory and regulatory requirements related to information technology and digital governance.

3. SCOPE

This Policy applies to:

- Students
- Faculty Members
- Administrative Staff
- Technical Staff

- Research Scholars
- Consultants
- Contract Employees
- Service Providers
- Alumni (where applicable)
- Authorized External Users

The Policy covers all digital systems, applications, databases, networks, cloud services, websites, portals, digital repositories, and information assets owned, managed, or utilized by the Institution.

4. DIGITAL GOVERNANCE FRAMEWORK

The Institution shall establish an integrated digital governance framework to support academic, administrative, research, financial, and student support functions.
The framework shall include:

- E-Governance Systems
- Enterprise Resource Planning (ERP)
- Learning Management System (LMS)
- Digital Documentation Systems
- Institutional Websites and Portals
- Data Management Systems
- Cyber security Framework
- Digital Communication Platforms
- Digital Content Management Systems

Digital governance initiatives shall aim to improve operational effectiveness, transparency, and stakeholder satisfaction.

5. E-GOVERNANCE

The Institution shall promote the use of digital technologies for governance, administration, teaching-learning, examinations, finance, human resources, student services, and institutional communication.
E-governance initiatives may include:

- Online Admissions
- Student Information Systems
- Faculty Information Systems
- Examination Management Systems
- Financial Management Systems
- Human Resource Management Systems
- Electronic Document Management Systems
- Online Grievance Redressal Systems

The Institution shall continuously enhance digital processes to improve efficiency and service delivery.

6. DATA PROTECTION AND PRIVACY

The Institution shall protect the confidentiality, integrity, and availability of institutional information assets.
Data protection measures shall include:

- Controlled Access to Information
- User Authentication Mechanisms
- Role-Based Access Control
- Secure Data Storage
- Data Backup and Recovery
- Data Retention and Disposal Procedures
- Privacy Protection Measures

Personal information of students, faculty, staff, alumni, and stakeholders shall be collected, processed, stored, and utilized only for legitimate institutional purposes.
Unauthorized access, disclosure, modification, or misuse of data shall be prohibited.

7. CYBER SECURITY

The Institution shall establish and maintain a comprehensive cyber security framework to safeguard digital infrastructure and information assets.
Cyber security measures may include:

- Firewall Protection
- Intrusion Detection and Prevention Systems
- Endpoint Security Solutions
- Antivirus and Anti-Malware Protection
- Vulnerability Assessment
- Security Audits
- Multi-Factor Authentication
- Secure Network Management
- Cyber security Awareness Programmes

The Institution shall periodically review and strengthen Cyber security measures to address emerging threats and vulnerabilities.

8. ENTERPRISE RESOURCE PLANNING (ERP)

The Institution shall utilize ERP systems for integrated management of academic, administrative, financial, and student-related processes.
ERP modules may include:

- Admissions
- Student Records
- Academic Management
- Attendance Management
- Examination Management
- Finance and Accounts
- Human Resources
- Inventory Management
- Hostel Management

- Transport Management

All users shall ensure accuracy, confidentiality, and responsible use of ERP data.
Unauthorized access, sharing of credentials, or manipulation of ERP records shall be prohibited.

9. LEARNING MANAGEMENT SYSTEM (LMS)

The Institution shall maintain a Learning Management System (LMS) to support technology-enabled teaching and learning.
The LMS may facilitate:

- Course Content Delivery
- Assignment Submission
- Assessment and Evaluation
- Discussion Forums
- Student Progress Monitoring
- Online Learning Activities
- Academic Resource Sharing

Faculty members shall ensure timely updating of learning resources and academic activities within the LMS.
Students shall utilize LMS resources responsibly and comply with institutional guidelines.

10. DIGITAL CONTENT GOVERNANCE

The Institution shall encourage the development, management, dissemination, and preservation of quality digital content.
Digital content may include:

- E-Learning Materials
- Lecture Videos
- Digital Libraries
- Research Repositories
- Educational Resources
- Institutional Publications
- Multimedia Content
- Online Course Materials

Digital content shall:

- Maintain academic integrity.
- Respect intellectual property rights.
- Comply with copyright requirements.
- Promote accessibility and inclusivity.
- Align with institutional values and objectives.

11. WEBSITE AND DIGITAL COMMUNICATION MANAGEMENT

The Institution shall maintain official websites, portals, and digital communication platforms to facilitate dissemination of authentic information.
Content published on institutional platforms shall:

- Be accurate and current.

- Be approved by the competent authority.
- Comply with institutional policies.
- Avoid discriminatory, offensive, or misleading content.

The Institution reserves the right to modify, remove, or restrict content that violates applicable policies or regulations.

12. DIGITAL RECORDS MANAGEMENT

The Institution shall establish mechanisms for the creation, storage, retrieval, retention, archiving, and disposal of digital records.

Digital records shall be maintained in accordance with:

- Regulatory Requirements
- Accreditation Requirements
- Institutional Policies
- Data Protection Principles

Appropriate backup and recovery mechanisms shall be implemented to ensure business continuity.

13. DIGITAL ETHICS AND RESPONSIBLE USE

All users shall:

- Use digital resources ethically and responsibly.
- Respect privacy and confidentiality.
- Protect passwords and access credentials.
- Avoid unauthorized access to systems and information.
- Comply with applicable laws and institutional regulations.

The use of digital systems for unlawful, fraudulent, offensive, or harmful activities shall be prohibited.

14. GOVERNANCE FRAMEWORK

The implementation of this Policy shall be overseen by:

- Executive Council
- Vice-Chancellor
- Pro Vice-Chancellor
- Registrar
- Director Administration
- IT Administrator
- Software Cell
- Website Management Committee
- IQAC
- Heads of Schools and Departments

These authorities shall ensure effective implementation, monitoring, security, compliance, and continuous improvement of digital governance systems.

15. ROLES AND RESPONSIBILITIES

IT Administrator

- Manage digital systems and services.
- Oversee Cyber security and digital infrastructure.
- Ensure security and system availability.
- Coordinate technical support.

Software Cell

- Maintain ERP, LMS, and institutional applications.
- Provide user support and training.

Users

All users shall:

- Comply with this Policy.
- Protect institutional information assets.
- Report security incidents promptly.
- Utilize digital resources responsibly.

16. COMPLIANCE AND VIOLATION

Violation of this Policy may 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 digital resources.

17. MONITORING AND AUDIT

Periodic audits, security assessments, system reviews, compliance evaluations, and performance assessments shall be conducted to ensure effective implementation of this Policy. Corrective and preventive actions shall be undertaken wherever required.

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.

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.

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