IT Policy

Sai Tirupati University

Ambua Road, Village Umarda, Girwa, Udaipur - 313015 (Raj.)

www.saitirupatiuniversity.ac.in | info@saitirupatiuniversity.ac.in

0		Issued for Implementation
Rev.	Date:	Description
SAI TIRUPATI UNIVERSITY UDAIPUR		IT Policy

SAI TIRUPATI UNIVERSITY PRESIDENT (VC) SAI*UDAIPUR

IT Policy

Introduction

The Information Technology (IT) Policy at Sai Tirupati University, Umarda, Udaipur is designed to ensure the effective, secure, and ethical use of IT resources. This policy outlines the principles, guidelines, and responsibilities for the use of the university's IT infrastructure, ensuring that it supports the institution's academic, administrative, and research activities while maintaining high standards of security and integrity.

Objectives

The primary objectives of the IT Policy are:

- To protect the university's IT infrastructure and data from unauthorized access, breaches, and other security threats.
- To encourage the ethical use of IT resources in alignment with the university's values and legal requirements.
- To ensure efficient and effective use of IT resources in support of the university's mission and goals.
- To provide reliable and secure access to IT resources for students, faculty, and staff.
- To ensure IT resources effectively support the academic, research, and administrative functions of the university.

Scope

This policy applies to all users of IT resources at Sai Tirupati University, Umarda, Udaipur, including students, faculty, staff, contractors, and visitors. IT resources include, but are not limited to, computers, servers, networks, software, data, and other digital resources.

IT Governance

1. IT Governance Structure

- The university shall establish an IT Governance Committee to oversee the implementation and management of the IT Policy.
- The IT Governance Committee shall include representatives from the administration, faculty, staff, and IT department.
- The committee shall be responsible for developing and reviewing IT policies, setting IT priorities, and ensuring alignment with the university's strategic goals.

2. Roles and Responsibilities

2.1 IT Department

- The IT Department shall be responsible for the implementation, maintenance, and support of IT infrastructure and services.
- The IT Department shall provide technical support, manage IT projects, and ensure the security of IT resources.

2.2 Users

- Users of IT resources are responsible for using these resources ethically and in compliance with the IT Policy.
- Users must protect their login credentials, report security incidents, and adhere to the university's IT usage guidelines.

2.3 IT Governance Committee

Sai Tirupati University Udaipur

- The IT Governance Committee shall oversee the development and implementation of IT policies and procedures.
- The committee shall review and approve IT projects, budgets, and strategic plans.

IT Security

1. Network Security

1.1 Access Control

- Access to the university's network shall be controlled through authentication mechanisms, including passwords and multi-factor authentication.
- Network access shall be granted based on the principle of least privilege, ensuring users have access only to the resources necessary for their roles.

1.2 Firewalls and Intrusion Detection

- Firewalls and intrusion detection/prevention systems shall be deployed to protect the network from unauthorized access and threats.
- The IT Department shall regularly monitor and update these systems to address emerging threats.

1.3 Wireless Security

- Wireless networks shall be secured using strong encryption protocols and secure authentication methods.
- Guest access to wireless networks shall be provided separately from the internal network to maintain security.

2. Data Security

2.1 Data Classification

- Data shall be classified based on its sensitivity and importance, with appropriate security measures applied to each classification.
- The classification levels shall include public, internal, confidential, and restricted data.

2.2 Data Encryption

- Sensitive data shall be encrypted both in transit and at rest to protect it from unauthorized access and breaches.
- Encryption standards shall be regularly reviewed and updated to ensure they remain effective.

2.3 Data Backup and Recovery

- Regular backups of critical data shall be performed to ensure data can be recovered in case of loss or corruption.
- Backup and recovery procedures shall be tested periodically to ensure their effectiveness.

3. Endpoint Security

3.1 Antivirus and Antimalware

- All endpoint devices, including desktops, laptops, and mobile devices, shall have up-to-date antivirus and antimalware software installed.
- The IT Department shall regularly update and manage antivirus software to protect against new threats.

3.2 Patch Management

- Software and operating systems on endpoint devices shall be regularly updated with security patches and updates.

- Users shall be encouraged to install updates promptly to maintain security.

4. Incident Response

4.1 Incident Reporting

- Users shall report any IT security incidents, such as data breaches, malware infections, or unauthorized access, to the IT Department immediately.
- A clear incident reporting procedure shall be communicated to all users.

4.2 Incident Management

- The IT Department shall have an incident response plan in place to address and manage IT security incidents.
- The plan shall include procedures for identifying, containing, eradicating, and recovering from incidents.

IT Usage Guidelines

1. Acceptable Use

- IT resources shall be used for academic, research, and administrative purposes in alignment with the university's mission.
- Personal use of IT resources shall be limited and must not interfere with academic or administrative activities.

2. Prohibited Activities

- Users shall not engage in activities that violate the law, infringe on the rights of others, or compromise the security and integrity of IT resources.
- Prohibited activities include, but are not limited to, unauthorized access, distribution of malicious software, copyright infringement, and harassment.

3. Email and Communication

- Email and other communication tools provided by the university shall be used for official purposes.
- Users shall not send spam, chain letters, or other inappropriate messages using the university's communication tools.

IT Resource Management

1. Hardware and Software Management

1.1 Hardware Acquisition and Maintenance

- The acquisition of hardware shall be based on the university's needs and strategic priorities.
- The IT Department shall be responsible for the maintenance and support of hardware resources.

1.2 Software Licensing and Management

- All software used by the university shall be properly licensed and managed to ensure compliance with licensing agreements.
- The IT Department shall maintain an inventory of software licenses and ensure they are up to date.

2. IT Asset Management

- An inventory of all IT assets shall be maintained, including hardware, software, and network components.
- The IT Department shall regularly update the inventory and conduct audits to ensure accurate records.

IT Support and Training

1. **IT Support Services**

1.1 Help Desk

- The IT Department shall provide a help desk service to assist users with technical issues and inquiries.
- The help desk shall be accessible through multiple channels, including phone, email, and an online ticketing system.

1.2 Technical Support

- Technical support shall be available to address hardware and software issues, network connectivity problems, and other IT-related concerns.
- The IT Department shall prioritize support requests based on their urgency and impact on university operations.

2. **User Training and Awareness**

2.1 IT Training Programs

- The university shall offer IT training programs to enhance the digital literacy and technical skills of students, faculty, and staff.
- Training programs shall cover topics such as cybersecurity, software usage, and best practices for IT resource management.

2.2 Cybersecurity Awareness

- Regular cybersecurity awareness campaigns shall be conducted to educate users about potential threats and safe computing practices.
- The IT Department shall provide resources and guidelines on how to recognize and respond to cybersecurity threats.

IT Development and Innovation

1. **IT Project Management**

1.1 Project Planning and Approval

- IT projects shall be planned and approved based on the university's strategic goals and priorities.
- The IT Governance Committee shall review and approve major IT projects, ensuring they align with the institution's objectives.

1.2 Project Implementation

- IT projects shall be implemented using best practices in project management, including clear timelines, milestones, and deliverables.
- The IT Department shall ensure effective communication and collaboration among project stakeholders.

1.3 Project Evaluation

- The success and impact of IT projects shall be evaluated upon completion, with lessons learned documented for future reference.
- The IT Governance Committee shall review project evaluations and provide feedback for continuous improvement.

2. **Innovation and Research**

2.1 Encouraging Innovation

- The university shall encourage innovation in the use of IT resources to enhance teaching, learning, and administrative processes.

- Faculty and students shall be supported in developing and implementing innovative IT solutions.

2.2 Research and Development

- The IT Department shall collaborate with academic departments to support research and development activities related to IT.
- Opportunities for external funding and partnerships in IT research shall be explored.

Compliance and Monitoring

1. Policy Compliance

- All users of IT resources shall comply with the IT Policy and related guidelines.
- Non-compliance with the IT Policy may result in disciplinary action, including revocation of access to IT resources.

2. Monitoring and Auditing

2.1 Network and System Monitoring

- The IT Department shall monitor network and system activities to ensure the security and performance of IT resources.
- Monitoring activities shall be conducted in compliance with privacy regulations and ethical standards.

2.2 Regular Audits

- Regular audits of IT resources and practices shall be conducted to ensure compliance with the IT Policy and identify areas for improvement.
- Audit findings shall be reported to the IT Governance Committee and addressed promptly.

Data Management and Privacy

1. Data Privacy

1.1 Personal Data Protection

- Personal data of students, faculty, staff, and other stakeholders shall be protected in accordance with applicable data protection laws and regulations.
- The university shall implement measures to ensure the confidentiality, integrity, and availability of personal data.

1.2 Data Access and Sharing

- Access to personal data shall be restricted to authorized personnel only.
- Data sharing shall be conducted in compliance with data protection policies and with the explicit consent of the data subjects.

2. Data Retention and Disposal

2.1 Data Retention

- Data retention policies shall be established to determine the appropriate retention periods for different types of data.
- The university shall ensure that data is retained only for as long as necessary to fulfill its purposes and legal requirements.

2.2 Data Disposal

- Data that is no longer needed shall be disposed of securely to prevent unauthorized access and breaches.

- The IT Department shall implement procedures for the secure disposal of data, including digital and physical records.

Risk Management

1. Risk Assessment

- Regular risk assessments shall be conducted to identify and evaluate potential IT risks.
- The IT Department shall develop and implement risk mitigation strategies to address identified risks.

2. Business Continuity and Disaster Recovery

2.1 Business Continuity Planning

- The university shall develop and maintain a business continuity plan to ensure the continued operation of critical IT services in the event of a disruption.
- The plan shall include procedures for maintaining essential functions and services during emergencies.

2.2 Disaster Recovery Planning

- A disaster recovery plan shall be established to ensure the rapid recovery of IT services and data in the event of a disaster.
- The IT Department shall regularly test and update the disaster recovery plan to ensure its effectiveness.

Communication and Policy Review

1. Communication of the IT Policy

- The IT Policy shall be communicated to all members of the university community through various channels, including the university website, email, and orientation sessions.
- Users shall acknowledge their understanding and acceptance of the IT Policy.

2. Policy Review and Updates

- The IT Policy shall be reviewed regularly to ensure its continued relevance and effectiveness.
- Updates to the IT Policy shall be approved by the IT Governance Committee and communicated to all users.

Conclusion

The IT Policy at Sai Tirupati University, Umarda, Udaipur is designed to ensure the secure, ethical, and effective use of IT resources. By adhering to the principles and procedures outlined in this policy, the university can support its academic, research, and administrative functions while maintaining high standards of security and integrity. This policy will be reviewed and updated regularly to ensure its continued relevance and effectiveness in meeting the university's IT needs.

Sai Tirupati University Udaipur

Approved By

Vice-Chancellor
Sai Tirupati University, Umarda, Udaipur

SAI TIRUPATI UNIVERSITY PRESIDENT (VC) SAI*UDAIPUR