Information Technology Policy and Procedure Manual
JSS Academy of Higher Education and Research

Table of Contents

Information Technology Policy and Procedure Manual 1
Introduction 3
Technology Hardware Purchasing Policy 4
Purpose of the Policy 4
Procedures 4
Policy for Getting Software 7
Purpose of the Policy 7
Procedures 7
Policy for Use of Software 9
Purpose of the Policy 9
Procedures 9
Bring Your Own Device Policy 12
Purpose of the Policy 12
Procedures 12
Information Technology Security Policy 16
Purpose of the Policy 16
Procedures 16
Information Technology Administration Policy 18
Purpose of the Policy 18
Procedures 18
Website Policy 19
Purpose of the Policy 19
Procedures 19
IT Service Agreements Policy 21
Purpose of the Policy 21
Procedures 21
Emergency Management of Information Technology 22
Purpose of the Policy 22
Procedures 22
Data Backup Policy 24

Purpose of the Policy 24
Procedures 24
Power Backup Policy 25
Purpose of the Policy 25
Procedures 25

Preamble

In this digital era, information technology plays a pivotal role in transforming the landscape of education, research, and administrative operations. JSS Academy of Higher Education & Research (JSS AHER) recognizes the significance of technology in fostering innovation, improving efficiency, and enhancing the overall academic experience for students, faculty, and staff. The Information Technology Policy of JSS AHER outlines the principles, guidelines, and best practices that govern the effective and responsible use of information technology resources within the institution.

This policy aims to establish a robust and secure IT infrastructure that enables seamless access to educational resources, fosters cutting-edge research, and streamlines administrative processes. It emphasizes the importance of data privacy, cybersecurity, and compliance with relevant laws and regulations in the digital domain. Additionally, the policy seeks to promote digital literacy and technology adoption among the academic community, empowering them to harness the full potential of information technology for academic and professional growth.

By adhering to this Information Technology Policy, JSS AHER endeavors to create a dynamic and inclusive technological environment, ensuring the confidentiality, integrity, and availability of digital resources while fostering a culture of innovation and excellence. This policy is a testament to our commitment to staying at the forefront of technological advancements and leveraging IT as a strategic enabler for achieving our academic and research goals.

Information Technology Policy of JSS Academy of Higher Education & Research highlights the significance of technology in today's educational landscape. It emphasizes the institution's commitment to providing a secure and cutting-edge IT infrastructure that enhances academic experience and supports research and administrative processes. The policy also underscores the importance of data privacy, cybersecurity, and digital literacy in ensuring responsible and effective IT usage.

Purpose & Scope

Purpose:

The purpose of the Information Technology Policy for JSS Academy of Higher Education & Research is to establish a comprehensive framework that governs the strategic planning, implementation, and responsible use of information technology resources within the institution. This policy aims to:

Enhance Academic Excellence: Foster an environment where technology is harnessed to enhance teaching, learning, and research, empowering students and faculty to excel in their academic pursuits.

Ensure Data Security & Privacy: Safeguard sensitive and confidential information through robust cybersecurity measures, data encryption, and adherence to applicable data protection laws.

Optimize Administrative Efficiency: Streamline administrative processes through the integration of innovative IT solutions, reducing paperwork and enhancing operational efficiency.

Foster Innovation & Collaboration: Encourage a culture of technological innovation, knowledge sharing, and collaboration among the academic community, promoting interdisciplinary research and creative exploration.

Enable Digital Learning Resources: Provide easy access to digital learning resources, e-libraries, and online repositories to facilitate self-directed and remote learning opportunities for students and faculty.

Support Cutting-Edge Research: Facilitate the use of advanced computing resources, research tools, and high-performance computing facilities to support research and innovation across various disciplines.

Promote Digital Literacy: Enhance digital literacy among students, faculty, and staff, empowering them to leverage technology effectively and responsibly in their academic and professional endeavors.

Scope:

The Information Technology Policy applies to all members of the JSS Academy of Higher Education & Research community, including students, faculty, staff, researchers, and anyone utilizing the institution's IT infrastructure. The policy covers all aspects related to the acquisition, deployment, maintenance, and usage of information technology resources.

The scope of this policy includes, but is not limited to:

IT Infrastructure: Guidelines for the management and maintenance of the institution's hardware, software, networks, servers, and related infrastructure.

Data Security & Privacy: Measures to protect sensitive data, including personally identifiable information (PII), research data, and other confidential information, from unauthorized access or data breaches.

Responsible Use: Expectations for responsible and ethical use of IT resources, including compliance with copyright laws, software licenses, and acceptable use policies.

Digital Learning Resources: Guidelines for the development, accessibility, and usage of digital learning materials, e-libraries, and online educational platforms.

Research Computing: Policies and procedures for accessing and utilizing advanced computing resources for research purposes.

Cybersecurity: Measures to protect the institution's IT assets from cyber threats, malware, phishing, and other security risks.

Digital Literacy & Training: Initiatives to enhance digital literacy among the academic community and provide training on the effective use of IT tools and applications.

IT Governance: Establishing a governance framework to ensure effective decision-making, resource allocation, and alignment of IT initiatives with the institution's strategic goals.

The Information Technology Policy is subject to periodic review and updates to accommodate technological advancements, changing academic needs, and evolving IT security standards.

Technology Hardware Purchasing Policy

Policy Number: ITP - 01

Policy Date: 1/4/2019

IT hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners.

IT Hardware also includes to all the Networking related equipment like Routers, Switches, Access Points, Firewall, Servers etc.

Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the Institution to ensure that all hardware technology for the Organization is appropriate, value for money and where applicable integrates with other technology for the Organization. The objective of this policy is to ensure that there is standardization of IT hardware within the Organization and that the Organization would ensure that only the latest IT hardware is procured.

Procedures

Purchase of Hardware

Purchasing desktop computer systems

The Organization has made Microsoft Windows the standard Operating System for all the desktops except in case of specific project-based requirements of a different Operating System other than Windows.

The desktop computer systems must be purchased as standard desktop system bundle and must be from any one of the Manufacturers given below:

- HP
- Dell
- Lenovo

The desktop computer system bundle must include:

- Please refer – Standard IT Hardware Specification

The Desktop computer systems purchased must run Licensed Windows 10 or later Operating System.

Any change from the above requirements must be authorized by CIO and Approved by Registrar.

All purchases of desktops must be supported by Manufacturer's standard warranty and onsite support clauses.

All purchases must be in line with the Purchasing Policy of the Organization and the SOP on IT Asset Management.

Purchasing portable computer systems

The purchase of portable computer systems includes devices such as notebooks, laptops, tablets etc.

Portable computer systems purchased must run Licensed Windows 10 or later Operating System.

The portable computer systems purchased must be from any one of the manufacturers.

- HP
- Dell
- Lenovo

The standard configuration of the Portable System is as below:

Please refer – Standard IT Hardware Specification

Any change from the above requirements must be authorized by the CIO and approved bythe Registrar.

All purchases of desktops must be supported by Manufacturer's standard warranty and onsite support clauses.

All purchases must be in line with the Purchasing Policy of the Organization and the SOP on IT Asset Management.

Purchasing Server Systems

As part of the overall IT Roadmap, it is desired that most of the operations requiring IT Server infrastructure be met by the Cloud Service Provider like Microsoft Azure. In very rare cases like setting up the Network Infrastructure for DHCP, DNS etc., local servers can be deployed.

Server systems can only be purchased by the IT Department of the Institution.

Purchasing computer peripherals

Computer system peripherals include add-on devices such as printers, scanners, external hard drives etc.

Computer peripherals can only be purchased where they are not included in any hardware purchase or are an additional requirement to existing peripherals.

Computer peripherals purchased must be compatible with all other computer hardware and software in the Organization.

The purchase of computer peripherals can only be authorized by the IT Department.

All purchases must be in line with the Purchasing Policy of the Organization and the SOP on IT Asset Management.

Policy for Getting Software

Policy Number: ITP - 02

Policy Date: 1/4/2019

Purpose of the Policy

This policy provides guidelines for the purchase of software for the Organization to ensure that all software used by the Organization is appropriate, value for money and where applicable integrates with other technology for the Organization. This policy applies to software obtained as part of hardware bundle or pre-loaded software or Application Software as part of Software as a Service offering, Applications Customized for JSS.

Procedures

Request for Software

All software, including all commercial and non-commercial software such as open source, freeware, etc. must be approved by CIO and/or Registrar prior to the use or download of such software. The request for procurement or commissioning of any software is to be made to IT Department of the Organization and only upon approval the implementation to be taken up.

Purchase of software

The purchase of all software must adhere to this policy.

All purchased software must be purchased by the IT Department. All purchases must be in line with the Purchasing Policy of the Organization and the SOP on IT Asset Management.

Obtaining open source or freeware software

As Open source or freeware software can be obtained without payment and usually downloaded directly from the internet, utmost care much be exercised to understand and adhere to the Licensing requirements of the Software. Wherever Open Source or Freeware software is required to be installed, due approvals much be taken from CIO and/or Registrar before installation and use.

Any change from the above requirements must be authorized by the CIO and/or Registrar.

Additional Policies for Custom Software Solutions and SAAS Application and the Web Site

Purchasing Policy

Custom made Software or Application and the Application offered as Software as a Service and developments around Organizations Web Site can only be procured or contracted by the IT Department in view of the complications arising out of interfaces and Technology interoperability issues. No deviation is accepted in purchasing or procuring such an application.

In cases where it is essential to obtain or custom make such applications, requesters are to provide a business case on the need for such an application and the IT Department would work with the identified vendors to host or deliver such an application.

All purchases must be in line with the Purchasing Policy of the Organization and the SOP on IT Asset Management.

Policy for Use of Software

Policy Number: ITP - 03

Policy Date: 1/4/2019

Purpose of the Policy

This policy provides guidelines for the use of software for all employees and students within the Organization to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

Procedures

Software Licensing

All computer software copyrights, and terms of all software licenses will be followed by all employees of the Organization.

Where licensing states limited usage (i.e., number of computers or users etc.), then it is the responsibility of the individual Department or Constituent College to ensure these terms are followed.

IT Department Staff are authorized and responsible to conduct and completing a software audit of all Software once a year to ensure that software copyrights and license agreements are adhered to.

Software Installation

All software must be appropriately registered with the supplier where this is a requirement. JSS

Academy of Higher Education and Research is to be the registered owner of all software.

Only software obtained in accordance with the getting software policy is to be installed on the Organization’s computers.

All software installation is to be carried out by the IT Department or in consultation with the IT Department.

All software to be used should be licensed and no pirated software to be installed in any system belonging to the organization. Software upgrades shall not be carried out on a computer that does not already have a copy of the original version of the software loaded on it.

Software Usage

Only software purchased in accordance with the policy is to be used within the Organization.

Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All employees must receive training in all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of the respective HR Department of the Constituent Colleges.

Employees are prohibited from bringing software from home and loading it onto the Organization's computer hardware.

Unless express approval from CIO and/or Registrar is obtained, software cannot be copies or installed on employees' home computer.

Unauthorized software is prohibited from being used in the Organization. This includes the use of software owned by an employee and used within the Organization.

Duplicating, acquiring or use of pirated software copies is prohibited. Any employee who makes, acquires, or uses unauthorized copies of software will be referred to the CIO for disciplinary actions. The illegal duplication of software or other copyrighted works is not condoned within this Organization and the CIO is authorized to undertake disciplinary action where such an event occurs.

Breach of Policy

Where there is a breach of this policy by an employee or student, that employee or student will be referred to an IT Committee for disciplinary action.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify the IT Department immediately. If the breach is not reported, and it is determined that an employee failed to report the breach, then that employee will be referred to an IT Committee disciplinary actions.

Additional Policies for Use of Software

It is requested to read this policy along with JSSU IT Policy- Acceptable Use of Information Systems.

Bring Your Own Device Policy

Policy Number: ITP - 04

Policy Date: 1/4/2019

At JSS we acknowledge the importance of mobile technologies in improving Organization communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to JSS's network and equipment. We encourage you to read this document in full and to act upon the recommendations. This policy should be read and carried out by all staff along with JSSU IT Policy - Acceptable Use of Information Systems.

Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets, and other types of mobile devices for Organization purposes. All staff who use or access JSS's technology equipment and/or services are bound by the conditions of this Policy along with JSSU IT Policy- Acceptable Use of Information Systems.

Procedures

Current mobile devices approved for Organization use.

The following personally owned mobile devices are approved to be used for Organization purposes:

- Mobile devices such as notebooks, smart phones, tablets, iPhone, removable media.

Current devices are strictly prohibited from use within the Organization's Network.

- Routers, Switches, Modems, and other networking gadgets which interfere withthe Organizations Network.

Registration of personal mobile devices for Organization use

Employees when using personal devices for Organization use will register the device with the ITDepartment through the JSSUOnline Portal by providing the MAC ID of the device.

The IT Department will record the device and can track the utilization of resources by the device and may block the device in case the policy JSSU IT Policy- Acceptable Use of Information Systemsis breached.

Personal mobile devices can only be used for the following Organization purposes:

- Use such as email access, Organization internet access, Organizations Web basedApplications, Organization telephone calls etc.

Each employee who utilizes personal mobile devices agrees:

- Not to download or transfer Organization or personal sensitive information to the device. Sensitive information includes for example intellectual property, Employee details, Projects being approved, executed etc.

- Not to use the registered mobile device as the sole repository for JSS's information. All Organization information stored on mobile devices should be backed up on to Organizations IT Assets.

- To make every reasonable effort to ensure that JSS's information is not compromised using mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorized persons and all registered devices should be password protected.

- To maintain the device with the latest software, Anti-Virus Software etc.

- Backup important documents on to the Company Cloud Storage provided periodicallyand ensure availability all the time.

- Not to share the device with other individuals to protect the Organization data access through the device.
- To abide by JSSU IT Policy- Acceptable Use of Information Systems for appropriate use and access of internet sites etc.
- To notify JSS immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an untrusted or unknown source to JSS's equipment.

All employees who have a registered personal mobile device for Organization use acknowledge that the Organization:

- Owns all intellectual property created on the device.
- Can access all data held on the device, including personal data.
- Can ask the user to regularly back-up data held on the device.
- Can delete all data held on the device in the event of loss or theft of the device.
- Can delete all data held on the device upon termination of the employee.
- Has the right to deregister the device at any time.

Keeping mobile devices secure

The following must be observed when handling mobile computing devices (such as notebooks and iPads):

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away.
- Cable locking devices should also be considered for use with laptop computers in public places, e.g., in a seminar or conference, even when the laptop is attended
- Mobile devices should be carried as hand luggage when travelling by aircraft.

Exemptions

This policy is mandatory unless granted an exemption by the Organizations Authority. Any requests for exemptions from any of these directives should be referred to the CIO.

Breach of this policy

Any breach of this policy will be referred to the CIO who will review the breach and determine adequate consequences, which can include measures such as confiscation of the device and or termination of grant of access to the device from Organizations Network.

Indemnity

JSS bears no responsibility whatsoever for any legal action threatened or started due to the conductand activities of staff or students in accessing or using these resources or facilities. All staff and students indemnify JSS against all damages, costs and expenses suffered by JSS arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by JSS.

Information Technology Security Policy

Policy Number: ITP - 05

Policy Date: 1/4/2019

Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the Organization to ensure integrity, confidentiality and availability of data and assets. This policy is to be read along with JSSU IT Policy- Acceptable Use of Information Systems.

Procedures

Physical Security

The Organizations Data Centre housing Servers, and other network assets, are secured with adequate ventilation and appropriate access through relevant security measures such as Lock and Key, Manned Security Personnel etc.

It will be the responsibility of the IT Department to ensure that this requirement is always followed. Any employee becoming aware of a breach of this security requirement is obliged to notify the IT Department immediately.

All security and safety of all portable technology, such as laptop, notepads, iPad etc. will be the responsibility of the employee who has been issued with such an IT Asset. Each employee is required to use locks, passwords, etc. and to ensure the asset is always kept safely to protect the security of the asset issued to them.

In the event of loss or damage, the IT Department will assess the security measures undertaken to determine if the employee will be required to reimburse the Organization for the loss or damage.

All IT Assets such as laptop, notepads, iPads etc. when kept at the office desk is to be secured by relevant security measure, such as keypad, lock etc.

Information Security

All Sensitive, Valuable, or Critical Organization data to be backed up regularly to safeguard Organizations Interest.

It is the responsibility of individual Employee to ensure that data back-ups are conducted regularly and the backed-up data is kept safe.

All technology that has internet access must have anti-virus software installed. It is the responsibility of the IT Department to install all anti-virus software and ensure that this software remains up to date on all technology used by the Organization.

Data and Information used within the Organization to adhere to the privacy laws and the Organization's confidentiality requirements. Any employee breaching this will be liable for disciplinary actions.

Technology Access

Every employee will be issued with a unique identification code to access the Organization technology and application and will be required to maintain confidentiality of the same.

Information Technology Administration Policy

Policy Number: ITP - 06

Policy Date: 1/4/2019

Purpose of the Policy

This policy provides guidelines for the administration of information technology assets and resources within the Organization.

Procedures

All software installed, and the license information must be registered with the IT Department Database. It is the responsibility of the IT Department to ensure that this DB is maintained. The DB must record the following information:

- What software is installed on every machine.
- What license agreements are in place for each software package.
- Renewal dates if applicable.

CIO is responsible for the maintenance and management of all service agreements for the Organization technology. Any service requirements must first be approved by the CIO and/or Registrar.

The IT Department is responsible for maintaining adequate technological spare parts and other requirements including requirements such as Network Access Points, Switches, Routers etc.

A technology audit is to be conducted by the IT Committee to ensure that all information technology policies are being adhered to.

Any unspecified technology administration requirements should be directed to the CIO.

Website Policy

Policy Number: ITP - 07

Policy Date: 1/4/2019

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related tothe Organization website and regular Updates.

Procedures

Website Register

The Organization Website register (Soft Copy Register – JSS - Website and JSSUOnline Hosting Details) must record the following details:

- List of domain names registered to the Organization.
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

Keeping the register up to date will be the responsibility of the IT Department. The

CIO will be responsible for any renewal of items listed in the register.

Website Content

All content on the Organization website is to be accurate, appropriate and current. This will be the responsibility of the individual Content Providers, Constituent Colleges and Departments who provide the Content.

All content on the website must be approved by the respective owners of the Content.

The content of the website is to be reviewed by a Web Site Committee to be constituted by respective Colleges and Departments of the Organization.

Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the Organization.

IT Service Agreements Policy

Policy Number: ITP - 08

Policy Date: 1/4/2019

Purpose of the Policy

This policy provides guidelines for all IT service agreements entered into on behalf of the Organization.

Procedures

The following IT service agreements can be entered into on behalf of the Organization:

- Provision of general IT services – Like Xerox, Printers, Scanners, Biometric devices etc.
- Provision of Network Hardware and Software
- Repairs and maintenance of IT equipment
- Provision of Organization software
- Website, Application - Design, Development, Hosting, and Maintenance etc.

All IT service agreements must be reviewed by the Finance Officer before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received by the IT Department, then the agreement must be approved by the Registrar and Signed by the CIO.

All IT service agreements, obligations and renewals must be recorded before the start of the agreement and recorded.

If there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to the IT Committee who will be responsible for the settlement of such dispute.

Emergency Management of Information Technology

Policy Number: ITP - 09

Policy Date: 1/4/2019

Purpose of the Policy

This policy provides guidelines for emergency management of all information technology within the Organization. This policy is to be read along with the Organizations JSS - Disaster Recovery and Contingency Planning Document.

Procedures

IT Hardware Failure

Where there is failure of any of the Organization's hardware, this must be referred to the IT Department immediately.

It is the responsibility of IT Department to initiate relevant actions that should be undertaken in the event of IT hardware failure.

It is the responsibility of IT Department to undertake tests on planned emergency procedures to ensure that all planned emergency procedures are appropriate and minimize disruption to Organization operations.

Please refer JSS - Disaster Recovery and Contingency Planning

Virus or other security breach

In the event that the Organization's information technology is compromised by software virus or a possible security breach such breaches are to be reported to the CIO, Registrar and VC immediately.

CIO is responsible for ensuring that any security breach is dealt with within a reasonable timeframe to minimize disruption to Organization operations.

Website Disruption

If Organization website is disrupted, the following actions must be immediatelyundertaken:

- IT Department / CIO to be notified.
- Management – Vice Chancellor and Registrar, Principals of all Constituent Colleges
- Other Parties to be informed for recovery actions are.
    - Website hosing partner
    - Website design and development teams
    - Backup and Recovery support teams

Data Backup Policy

Policy Number: ITP - 10

Policy Date: 1/4/2019

Purpose of the Policy

This policy provides guidelines for data backup of the Applications that are in use in the University. This policy is to be read along with the Organizations JSS - Disaster Recovery and Contingency Planning Document.

Procedures

Application Backup

University has all its Master and Transaction data related to Students & Staff under JSSUOnline hosted on Microsoft Azure Cloud platform which provides safety and security of both the Application and Data.

Automated Daily Backup procedures are configured.

It is the responsibility of IT Department to initiate relevant actions of restoration that should be undertaken in the event of the breakdown of the Application and loss of data.

It is the responsibility of IT Department to undertake tests on planned emergency procedures to ensure that all planned emergency procedures are appropriate and minimize disruption to Organization operations.

Please refer JSS - Disaster Recovery and Contingency Planning

Backup of Standalone Systems

As far as possible all Staff have to keep their important working files on the Cloud Drive given to minimize the instances of data loss in case of hardware failure / theft of their systems.

It is the responsibility of the Users of the system to ensure that backup of the standalone systems done in accordance with the IT Policies and ensure safety of Organization’s data.

Power Backup Policy

Policy Number: ITP - 11

Policy Date: 1/4/2019

Purpose of the Policy

This policy provides guidelines for Poser Backup of the Computer Appliances that are in use in the University. This policy is to be read along with the Organizations JSS - Disaster Recovery and Contingency Planning Document.

Procedures

Central Power Backup

JSS AHER has made provision of 24 hr. power backup with installations of Power Generators for all the buildings on the Campus. In addition to the Power Generator, all Computer-related accessories are powered by suitable Uninterrupted Power Supplies at each Building.

It is the responsibility of the IT Department to initiate procurement and installation of suitable UPS systems as per standards.

Please refer JSS - Disaster Recovery and Contingency Planning

All University Computers and its accessories should be connected to only UPS power and under no circumstances connected to raw electricity power.

Review:

The Information Technology Policy of JSS Academy of Higher Education & Research shall be subject to regular review to ensure its relevance, effectiveness, and alignment with the institution's evolving technological landscape and strategic objectives. The policy review shall be conducted at least once every three years or as deemed necessary by the IT Steering Committee and the Office of Information Technology.

The review process shall involve the following steps:

1.Data Collection: The IT Steering Committee and the Office of Information Technology shall gather feedback and insights from key stakeholders, including students, faculty, staff, researchers, and IT administrators, to identify areas that require improvement or modification.

2. Technological Advancements: The policy review shall consider emerging technologies, trends, and best practices in the field of information technology to ensure that the institution remains at the forefront of digital innovation.

3. Legal and Regulatory Compliance: The policy review shall evaluate changes in relevant laws, regulations, and industry standards pertaining to data privacy, cybersecurity, intellectual property, and other IT-related matters, ensuring continued compliance.

4. Feedback Mechanism: A feedback mechanism shall be established to encourage members of the academic community to provide suggestions, concerns, and recommendations regarding the policy.

1.5. Comparative Analysis: The IT Steering Committee and the Office of Information Technology shall conduct a comparative analysis with similar IT policies in peer institutions and leading organizations to benchmark JSS AHER's practices.

6. IT Security Assessment: The policy review shall include an assessment of the institution's IT security measures, vulnerability scans, and risk analysis to strengthen cybersecurity protocols.

Amendment:

Amendments to the Information Technology Policy may be proposed at any time to address emerging IT challenges, accommodate technological advancements, or reflect changes in the institution's strategic priorities. The process for amendment shall follow these steps:

1. Proposal: Any member of the JSS AHER community may propose an amendment to the policy by submitting a formal proposal outlining the rationale, scope, and intended outcomes of the change.

2. Evaluation: The IT Steering Committee and the Office of Information Technology shall evaluate the proposed amendment in consultation with relevant stakeholders, considering its impact on academic, research, and administrative activities.

3. Approval: After thorough evaluation, the proposed amendment shall be presented to the Institutional Executive Committee for approval. Once approved, the amendment will become an integral part of the Information Technology Policy.

4. Communication: Following approval, the amended policy shall be communicated to all members of the academic community through official channels, including the institution's website, internal circulars, and email communications.

5. Implementation: The Office of Information Technology shall be responsible for implementing the approved amendments and ensuring their effective integration into the IT practices of the institution.

The Information Technology Policy, with its regular review and flexible amendment process, reinforces JSS AHER's commitment to maintaining a dynamic, secure, and cutting-edge technology environment that optimizes academic excellence, research productivity, and administrative efficiency.

The JSS Academy of Higher Education and Research (JSS AHER) IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the Organization including all the constituent colleges which must be followed by all staff and students as applicable. It also provides guidelines JSS AHER will use to administer these policies, with the correct procedure to follow.

JSS AHER will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures to be relevant in the changing scenario. These policies and procedures apply to all employees and students unless otherwise stated.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome. Please write to cio@jssuni.edu.in for suggestions on the IT Policies and Procedures.

In coordination with the Office of the Registrar and Vice Chancellor, the Chief information Officer of the Information Technology (IT) Division shall be responsible for the implementation and enforcement of the Information Technology Policy of JSS AHER .

These policies will be reviewed periodically to assess their effectiveness and relevance in promoting academic integrity. Necessary amendments will be made based on feedback and changing academic standards.

Date of Implementation: 01.06.2016
Date of Last Review: 01.06.2023
Date for Next Review:01.06.2026

REGISTRAR
Registrar
JSS Academy of Higher Education &
Sri Shivarathreeshwara N
Mysuru-570015