# SHRI MADHWA VADIRAJA INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(A unit of Shri Sode Vadiraja Mutt Education Trust ®)
VISHWOTHAMA NAGARA, BANTAKAL, UDUPI

An Affiliated Institution

Affiliated to VTU, Belagavi, Approved by AICTE, New Delhi

Accredited by NBA (BE – CSE, ECE) and NAAC with 'A' Grade

SMVITM

# IT POLICY AND GUIDELINES

SMVITM * BANTAKAL - 574 115 *

Principal
SHRI MADHWA VADIRAJA
INSTITUTE OF TECHNOLOGY & MANAGEMENT
Vishwothama... Dist.
BANTAKAL - 574 115

# Table of Contents


1. Introduction to IT policy ..... 1

Introduction: ..... 1

Objective of the IT Policy: ..... 1

Scope: ..... 2

Acceptable Use: ..... 2

Security: ..... 2

Privacy: ..... 2

Enforcement: ..... 2

Conclusion: ..... 2

2. Roles and Responsibilities of IT Administrator ..... 3

Introduction: ..... 3

Scope: ..... 3

Responsibilities: ..... 3

Strategic Planning: ..... 3

Infrastructure Management: ..... 3

Systems Administration: ..... 3

Vendor Management: ..... 4

Disaster Recovery and Business Continuity: ..... 4

Budgeting and Resource Allocation: ..... 4

Leadership and Team Management: ..... 4

Principal Approval: ..... 4

Enforcement: ..... 4

Conclusion: ..... 4

3. Software Installation and Licensing Policy ..... 5

Introduction: ..... 5

Scope: ..... 5

Responsibilities: ..... 5

Software Installation Procedures: ..... 5

Software Licensing Procedures: ..... 6

Security and Safety Considerations: ..... 6

Training and Documentation: 6
Conclusion: 6
4. Network Use Policy 7
Introduction: 7
Scope: 7
Responsibilities: 7
Acceptable Use: 7
Social Media Usage: 7
Network Access Duration: 7
Security: 7
Resource Usage: 8
Monitoring: 8
Enforcement: 8
Conclusion: 8
5. Email Account Use Policy 8
Scope: 8
Responsibilities: 8
Email account formats: 9
Email Account Provisioning and Termination: 9
Acceptable Use: 9
Security: 9
Retention and Disposal: 9
Monitoring: 9
Enforcement: 9
6. General Guidelines for Desktop Users Policy 10
Introduction: 10
Security: 10
Updates: 10
Backups: 10
Password Management: 10
Web Browsing: 10
Email: 10

File Management: 10
Hardware Maintenance 10
Energy Conservation: 10
Data Privacy: 10
Training and Support: 10
Compliance: 11
Prohibition of Pirated Software: 11
Conclusion: 11
7. IT Hardware Installation Policy 11
Introduction: 11
Scope: 11
Responsibilities: 11
Installation Procedures: 11
Security and Safety Considerations: 11
Training and Documentation: 12
Strict Action on Violations: 12
Conclusion: 12
8. General Guidelines for Website 12
Responsibility: 12
Faculty Members' Responsibilities: 12
Design and Development: 12
Quality Control: 12
Accessibility and User Experience: 13
Security: 13
Compliance: 13
Regular Reporting: 13
Process: 13
Active Webmaster Engagement: 13
Conclusion: 13
9. Incident Response and Reporting Policy: 14
Introduction: 14
Scope: 14

Incident Reporting: ..... 14
Incident Response Process: ..... 14
Incident Resolution: ..... 15
Incident Review and Analysis: ..... 15
Conclusion: ..... 15
10. Data Security Policy: ..... 15
Introduction: ..... 15
Confidentiality of Institutional Data: ..... 16
Ownership of Academic Documents/Data: ..... 16
Integrity and Manipulation of Institutional Data: ..... 16
Data Access and Permissions: ..... 16
Data Handling and Storage: ..... 16
Data Retention and Disposal: ..... 17
Conclusion: ..... 17
11. Acceptable Use Policy (AUP): ..... 17
Introduction: ..... 17
Scope: ..... 17
Acceptable Use: ..... 17
Conclusion: ..... 18
12. Software Development and Change Management Policy: ..... 18
Introduction: ..... 18
Scope: ..... 19
Software Developer Responsibilities: ..... 19
Software Change Management Process: ..... 19
Webmaster Responsibilities: ..... 20
Faculty Member Responsibilities: ..... 20
Conclusion: ..... 20
13. Social Engineering and Phishing Awareness Policy: ..... 20
Introduction: ..... 20
Scope: ..... 20
Awareness Training: ..... 21
Identification of Social Engineering Attacks: ..... 21

Response and Reporting: 21
Preventive Measures: 21
Compliance and Enforcement: 22
Conclusion: 22
14. Compliance and Regulatory Policy: 22
Introduction: 22
Scope: 22
Legal and Regulatory Compliance: 22
Data Protection and Privacy: 23
Intellectual Property and Copyright: 23
Compliance Reporting and Monitoring: 23
Training and Awareness: 23
Enforcement and Consequences: 24
Conclusion: 24

# 1. Introduction to IT policy

**Introduction:** Sri Madhwa Vadiraja Institute of Technology and Management (SMVITM) acknowledges the pivotal role of Information Technology (IT) in modern educational settings. As an institution dedicated to academic excellence and technological advancement, SMVITM is committed to fostering the responsible use of IT resources for the benefit of its entire community. This IT Policy delineates the guidelines and principles governing the utilization of IT resources within the institution.

**Objective of the IT Policy:** The primary objective of the IT Policy at SMVITM is to establish clear guidelines and procedures for the management, utilization, and maintenance of information technology resources within the institution. This policy serves as a framework for decision-making and ensures the efficient, effective, and secure utilization of IT resources. Specific objectives include:

1. Protecting the institution's information and technology assets from unauthorized access, use, or disclosure.
2. Ensuring compliance with pertinent laws, regulations, and industry standards related to information technology.
3. Promoting the effective and efficient use of IT resources to support academic and administrative functions.
4. Encouraging responsible and ethical use of IT resources by all members of the SMVITM community.
5. Establishing guidelines for the acquisition, installation, and maintenance of hardware and software.
6. Providing directives for the use of mobile devices and remote access to the institution's network.
7. Defining procedures for data backup and recovery, ensuring the integrity and availability of critical information.
8. Establishing protocols for incident response and disaster recovery to mitigate IT-related disruptions effectively.
9. Ensuring awareness of the IT policy among all employees, students, faculty, and contractors, along with their understanding of respective roles and responsibilities.

Overall, the IT Policy aims to promote the secure, reliable, and efficient utilization of IT resources to align with SMVITM's mission and objectives.

**Scope:** This policy applies to all individuals utilizing SMVITM's IT resources, including students, faculty, staff, and other stakeholders.

**Acceptable Use:** Users of SMVITM's IT resources are expected to utilize these resources responsibly, ethically, and lawfully. Prohibited activities include unauthorized access, theft or damage of IT resources, inappropriate use, hacking, distribution of illegal material or spam, personal gain, copyright infringement, or any activity contravening local, state, or federal laws.

**Security:** SMVITM is committed to safeguarding its IT resources and the data they contain. Users must protect their accounts and passwords from unauthorized access. The institution implements various security measures to counter external threats, and users are obligated to comply with all security policies and procedures.

**Privacy:** The privacy of users is paramount to SMVITM. Personal information collected by the institution is kept confidential and utilized solely for legitimate purposes. Users must adhere to all privacy policies and procedures.

Monitoring: SMVITM reserves the right to monitor its IT resources and users' activities in compliance with applicable laws and regulations. Appropriate action may be taken in response to policy violations.

**Enforcement:** Violations of this policy may result in disciplinary action, including suspension or termination of IT privileges, and may entail legal repercussions if the violation constitutes a criminal offense. SMVITM investigates all alleged policy violations and takes necessary action accordingly.

**Conclusion:** SMVITM is dedicated to promoting the responsible use of IT resources to facilitate academic and administrative endeavors. Compliance with this IT policy is mandatory for all users, and any breaches will be addressed with appropriate disciplinary measures. The institution reserves the right to revise this policy as needed to adapt to evolving technological landscapes and regulatory requirements.

## 2. Roles and Responsibilities of IT Administrator

**Introduction:** The IT Administrator at Sri Madhwa Vadiraja Institute of Technology and Management (SMVITM) plays a pivotal role in managing and maintaining the institution's IT infrastructure. This document outlines the key responsibilities and duties entrusted to the IT Administrator to ensure the smooth functioning of IT operations.

**Scope:** This policy applies specifically to the IT Administrator of SMVITM and delineates their roles and responsibilities in overseeing all aspects of the institution's IT systems and services.

**Responsibilities:** As the head of the IT department, the IT Administrator at SMVITM is responsible for a wide array of duties, including but not limited to:

### Strategic Planning:

1. Developing and implementing IT strategies aligned with the institution's goals and objectives.
2. Assessing emerging technologies and recommending innovative solutions to enhance efficiency and effectiveness.

### Infrastructure Management:

1. Overseeing the design, deployment, and maintenance of the institution's IT infrastructure, including networks, servers, and storage systems.
2. Ensuring the availability, reliability, and security of IT resources to support academic and administrative functions.

### Systems Administration:

1. Managing and administering servers, operating systems, and software applications to optimize performance and ensure seamless operation.
2. Implementing robust security measures to protect against cyber threats and unauthorized access.

User Support:

1. Providing technical support and assistance to faculty, staff, and students regarding IT-related issues, inquiries, and requests.
2. Facilitating training sessions and workshops to enhance end-user proficiency and awareness of IT systems and services.

Policy Development and Compliance:

1. Developing and enforcing IT policies, procedures, and guidelines to promote best practices, compliance with regulatory requirements, and adherence to security standards.

2. Monitoring and evaluating compliance with IT policies and initiating corrective actions as necessary.

### Vendor Management:

1. Managing relationships with IT vendors, service providers, and contractors to procure hardware, software, and services in accordance with institutional requirements and budgetary constraints.

2. Negotiating contracts, service level agreements (SLAs), and licensing agreements to ensure favorable terms and conditions.

### Disaster Recovery and Business Continuity:

1. Developing and implementing disaster recovery plans and business continuity strategies to minimize downtime and mitigate the impact of IT disruptions.

2. Conducting regular testing and drills to validate the effectiveness of contingency plans and identify areas for improvement.

### Budgeting and Resource Allocation:

1. Planning and allocating budgetary resources for IT projects, initiatives, and ongoing operations.

2. Monitoring expenditure, tracking costs, and optimizing resource utilization to maximize ROI and achieve cost-efficiency.

### Leadership and Team Management:

1. Providing leadership, direction, and mentorship to IT staff, fostering a collaborative and high-performance work environment.

2. Delegating tasks, assigning responsibilities, and conducting performance evaluations to ensure productivity and accountability.

**Principal Approval:** The IT Administrator must seek permission from the principal before making any major decisions that significantly impact the institution's IT operations and resources.

**Enforcement:** The IT Administrator is expected to fulfill their responsibilities diligently and in accordance with institutional policies and procedures. Failure to adhere to these responsibilities may result in disciplinary action, up to and including termination of employment.

**Conclusion:** The roles and responsibilities outlined in this document serve as a guideline for the IT Administrator at SMVITM in effectively managing the institution's IT resources and supporting its academic and administrative endeavors. By fulfilling these responsibilities with diligence and dedication, the IT Administrator contributes significantly to the success and advancement of SMVITM's IT initiatives and objectives.

## 3. Software Installation and Licensing Policy

**Introduction:** At SMVITM, we recognize the importance of efficiently managing software installations and licensing to ensure compliance, security, and optimal utilization of resources. This policy outlines the guidelines and procedures for the installation and licensing of software within our institution.

**Scope:** This policy applies to all faculty, staff, students, and contractors involved in the installation and licensing of software on devices owned or managed by SMVITM.

**Responsibilities:** The IT department at SMVITM is entrusted with the responsibility of overseeing all aspects of software installations and licensing compliance. Key responsibilities include:

- Ensuring all software installations adhere to this policy.
- Maintaining an up-to-date inventory of installed software and licenses.
- Providing technical assistance and guidance for software installations.
- Documenting all installation processes and configurations.

**Software Installation Procedures:** To ensure standardized and efficient software installations, the following procedures must be followed:

1. Submission of Installation Requests: Any individual requiring new software must submit a formal request to the IT department, detailing the software requirements and justification.
2. Review and Approval: The IT department will review each installation request to assess its necessity and feasibility.
3. Scheduling and Assignment: Upon approval, the IT department will schedule the installation and assign a qualified technician to carry out the task.
4. Installation and Configuration: The assigned technician will install the software according to manufacturer specifications and additional guidelines provided by the IT department.
5. Testing and Validation: Post-installation, the technician will thoroughly test the software to ensure proper functionality and integration with existing systems.
6. Documentation and Inventory Update: The IT department will update the software inventory and configuration records to reflect the new installation.

**Software Licensing Procedures:** SMVITM adheres to strict software licensing regulations to ensure legal compliance and avoid any potential licensing infringements. The following procedures govern software licensing:

1. License Inventory Management: The IT department maintains a comprehensive inventory of all software licenses owned by the institution.
2. License Verification: Prior to installation, the IT department verifies the availability of a valid license for the requested software.
3. Procurement and Extension: If a valid license is unavailable, the IT department procures the necessary licenses or obtains extensions from authorized vendors.
4. Documentation Maintenance: All software licenses, including agreements and proof of purchase, are diligently documented and stored securely by the IT department.

**Security and Safety Considerations:** To safeguard the integrity and security of our IT infrastructure, the following considerations are imperative during software installations:

1. Secure Installation Environment: Software installations must be conducted in secure environments to prevent unauthorized access.
2. Network Security: All software configurations must be aligned with network security policies to mitigate potential vulnerabilities.
3. Proper Software Disposal: Disposal of outdated software must adhere to SMVITM's software disposal policy to prevent data breaches and security risks.

**Training and Documentation:** All individuals involved in software installations and licensing procedures are required to undergo appropriate training on this policy and related protocols. The IT department is responsible for maintaining comprehensive documentation of all software-related activities, including requests, installation reports, and license records.

Enforcement: Any breaches or violations of this policy will be subject to investigation by the IT department. Depending on the severity of the violation, disciplinary actions may be taken, including but not limited to reprimand, suspension, or termination of employment or student status.

**Conclusion:** This Software Installation and Licensing Policy at SMVITM ensures the consistent and secure deployment of software across our institution's IT infrastructure. Compliance with this policy is crucial to maintaining the integrity, security, and efficiency of our IT systems. All members of the SMVITM community are expected to adhere to this policy and cooperate with the IT department to uphold these standards.

## 4. Network Use Policy

**Introduction:** At SMVITM, we recognize the significance of our computer network in facilitating academic and administrative activities. This policy delineates the guidelines and procedures governing the utilization of our organization's computer network.

**Scope:** This policy encompasses all network communications, encompassing both wired and wireless connections, and extends to all devices connected to SMVITM's network.

**Responsibilities:** All employees and contractors accessing SMVITM's network are entrusted with the responsibility of adhering to this policy in a responsible and ethical manner. The IT department is tasked with maintaining the network infrastructure, ensuring its proper configuration, and safeguarding its security.

**Acceptable Use:** The organization's network is primarily intended for business purposes. Limited personal use is permissible, provided it does not impede job performance or contravene this policy. Prohibited actions include:

1. Accessing or disseminating illegal content.
2. Sending or receiving messages containing offensive or inappropriate material.
3. Violating organizational policies or applicable laws.
4. Installing unauthorized software or utilizing unauthorized hardware, thereby creating security vulnerabilities.

**Social Media Usage:** Social media usage is restricted within SMVITM's network. Users desiring access to social media platforms must submit a request letter to the Administrator, providing a valid reason for access.

**Network Access Duration:** Network access is limited to 8 hours per session for all members of SMVITM. Users requiring continuous access without disconnection must submit an application to the Administrator, who will make the final decision in this regard.

**Security:** Users must exercise reasonable precautions to uphold network security and protect its data, including:

1. Employing strong passwords and periodically changing them.
2. Refraining from sharing passwords with others.
3. Abstaining from installing or utilizing unauthorized software or hardware.

4. Refraining from forwarding or sharing sensitive or confidential information without proper authorization.

5. Promptly reporting any suspicious or unauthorized activity to the IT department.

**Resource Usage:** Users must avoid excessive consumption of network resources, such as bandwidth or storage capacity, by:

1. Refraining from downloading or streaming large files or videos that consume excessive bandwidth.

2. Avoiding the storage of large files on the network without legitimate business justification.

**Monitoring:** SMVITM reserves the right to monitor network activity and usage for security, legal, or other business purposes.

**Enforcement:** Violations of this policy may result in disciplinary action, including termination of employment or contract termination. The IT department will conduct investigations into suspected violations and take appropriate actions as necessary.

**Conclusion:** This policy underscores the responsible and ethical utilization of SMVITM's network, emphasizing security and confidentiality. Compliance with this policy and its associated procedures is the collective responsibility of all employees and contractors.

## 5. Email Account Use Policy

Introduction: In fostering effective communication channels, our institution acknowledges the importance of a structured approach to email usage. This policy outlines the guidelines and procedures governing the utilization of email accounts within our organizational framework, ensuring seamless and secure correspondence.

**Scope:** This policy is applicable to all members, including employees, faculty, contractors, and students, who possess access to the institution's email system. It encompasses all email communications, irrespective of the sender's device or the recipient's affiliation.

**Responsibilities:** Users of the institution's email system are entrusted with the responsibility of adhering to this policy in a diligent and ethical manner. The IT department bears the responsibility of maintaining the email system's integrity, configuration, and security protocols.

**Email account formats:**

- For students: The email ID format is first name followed by the last 7 digits of their USN (University Serial Number) @sode-edu.in.
- For faculty: The email ID format is Firstnamelastname.branchcode@sode-edu.in.
- For other committee members or cells: Email IDs will be designated by the principal.

**Email Account Provisioning and Termination:** Each member is assigned a unique email ID within the institution's domain. For employees, email accounts will be deactivated one week following the cessation of their service. Similarly, for students, email accounts will be terminated six months after the completion of their engineering graduation course.

**Acceptable Use:** The institution's email system is designated exclusively for official purposes. Limited personal use is permissible, provided it does not disrupt professional obligations or contravene this policy. Prohibited actions include spamming, sending offensive content, violating intellectual property rights, or breaching organizational policies or laws.

**Security:** To uphold the security and confidentiality of email accounts and messages, users must employ robust password practices, refrain from password sharing, exercise caution when handling sensitive information, and promptly report any suspicious activity to the IT department.

**Retention and Disposal:** All email correspondence remains the property of the institution and must be retained or disposed of in accordance with the institution's records retention policy. Users are prohibited from deleting or altering email messages without proper authorization.

**Monitoring:** The institution reserves the right to monitor email communications for security, legal, or administrative purposes. Such monitoring may extend to personal email communications sent from institution-owned devices.

**Enforcement:** Violation of this policy may result in disciplinary action, including termination of employment or contract. Suspected breaches will be investigated by the IT department, which will take appropriate actions as necessary.

***Conclusion:*** This policy underscores the responsible and judicious use of email accounts within our institution, prioritizing security and confidentiality. Compliance with this policy is imperative for all members, and adherence to its provisions is essential for maintaining a conducive and professional communication environment.

## 6. General Guidelines for Desktop Users Policy

**Introduction:** Desktop computers play a vital role in academic and administrative functions at SMVITM. This policy outlines guidelines to ensure secure, efficient, and responsible desktop computer usage by all users.

**Security:**

1. Use strong passwords and enable two-factor authentication to safeguard accounts and data.

2. Install and regularly update antivirus and firewall software to mitigate malware and security threats.

**Updates:** Keep the operating system and software applications up-to-date with the latest security patches and updates to enhance performance and security.

**Backups:** Regularly backup important files and data to prevent loss in case of hardware failure or other issues.

**Password Management:** Utilize a password manager to securely store and manage passwords across different accounts.

**Web Browsing:** Exercise caution while browsing the internet; avoid visiting suspicious websites or downloading unknown files.

**Email:** Exercise caution when opening emails from unknown sources; refrain from clicking on links or downloading attachments from suspicious emails.

**File Management:** Organize and manage files and folders efficiently to ensure easy access and optimal storage space utilization.

**Hardware Maintenance:** Maintain cleanliness of desktops and peripherals to ensure optimal performance and prevent hardware issues caused by dust and debris.

**Energy Conservation:** Conserve energy and reduce electricity bills by turning off desktop computers and peripherals when not in use.

**Data Privacy:** Protect personal and sensitive data by utilizing encryption and secure file transfer protocols for sharing files and accessing sensitive information.

**Training and Support:** Seek training and support resources to enhance computer skills and troubleshoot encountered issues effectively.

**Compliance:** Ensure compliance with relevant regulations and organizational policies, including data protection laws and company policies on internet and computer use.

**Prohibition of Pirated Software:** Installation of pirated software is strictly prohibited. Users must contact the administrator to install/uninstall any applications.

**Conclusion:** This policy emphasizes adherence to guidelines for secure, efficient, and responsible desktop computer usage at SMVITM. It is the responsibility of all users to comply with these guidelines to maintain a safe and productive computing environment.

## 7. IT Hardware Installation Policy

**Introduction:** This policy delineates guidelines and procedures for the seamless installation of IT hardware within our organization. It is applicable to all IT hardware installations, whether undertaken by internal personnel or third-party contractors.

**Scope:** This policy extends to all employees and contractors involved in the installation of IT hardware within the organization.

**Responsibilities:** The IT department shoulders the responsibility of ensuring adherence to this policy during all IT hardware installations. This includes maintaining an updated inventory of all installed IT hardware, verifying proper configuration, and meticulously documenting the installation process.

### Installation Procedures:

1. All requests for IT hardware installation must be channeled through the IT department via our college's MIS software system, providing comprehensive details of the proposed installation.
2. The IT department will meticulously review each request to ascertain its necessity and feasibility.
3. Upon approval, the IT department will meticulously schedule the installation and designate a proficient technician for the task.
4. The designated technician will execute the installation in strict accordance with the manufacturer's specifications and any supplementary instructions provided by the IT department.
5. Post-installation, the technician will conduct thorough testing to ensure optimal functionality.
6. The IT department will promptly update the inventory and configuration records to reflect the newly installed hardware.

### Security and Safety Considerations:

1. All hardware installations must be conducted in a secure location to thwart unauthorized access.

2. To prevent electrical hazards, all hardware must be adequately grounded.
3. Hardware configurations must be meticulously verified to avert any compromise to network security.
4. Disposal of old hardware must adhere strictly to the organization's IT asset disposal policy.

**Training and Documentation:** All individuals involved in IT hardware installations must undergo comprehensive training on this policy and associated procedures. The IT department is tasked with maintaining meticulous documentation concerning IT hardware installations, encompassing requests, installation reports, and inventory records.

**Strict Action on Violations:** Any deviations from this policy will result in strict repercussions. Violators risk facing withdrawal of IT privileges and other disciplinary actions deemed necessary by the administration.

**Conclusion:** This policy underscores the paramount importance of uniform and secure IT hardware installations within our organization. By adhering to these guidelines, all employees and contractors contribute to maintaining the integrity and security of our IT infrastructure.

## 8. General Guidelines for Website

**Responsibility:** The institution's website serves as a crucial platform for disseminating information and fostering communication. The webmaster holds the responsibility for maintaining the website and its content. Any individual intending to publish web content must forward the details to the designated webmaster email ID. Upon review, the webmaster will make the decision regarding its publication on the institutional website. Additionally, the webmaster will add new web pages as per requests.

**Faculty Members' Responsibilities:** Faculty members are required to update their respective web pages with relevant information through the web accounts provided by the webmaster. Any dissemination of false or irrelevant information will result in strict action, including the permanent removal of the profile page from the website.

**Design and Development:** The webmaster, in collaboration with concerned coordinators or faculty members, will design new content, templates, portals, or pages to enhance the functionality and appeal of the website. This collaborative effort ensures that the website remains dynamic and meets the evolving needs of users.

**Quality Control:** The webmaster will ensure the quality and integrity of the website content by conducting periodic reviews and assessments. This includes verifying the accuracy and relevance of published content, as well as ensuring compliance with institutional standards and guidelines.

**Accessibility and User Experience:** The website will be designed and maintained to ensure accessibility for all users, including those with disabilities. User experience will be prioritized to facilitate easy navigation and seamless access to information.

**Security:** Stringent security measures will be implemented to safeguard the website against cyber threats and unauthorized access. Regular security audits and updates will be conducted to maintain the integrity of the website and protect sensitive data.

**Compliance:** All website content and functionality will comply with relevant laws, regulations, and institutional policies. This includes adherence to copyright laws, data protection regulations, and privacy policies.

### Regular Reporting:

After the successful completion of every institutional activity, it is imperative for the coordinators responsible for overseeing these activities to provide comprehensive reports to the webmaster. These reports serve as vital documentation of the event or initiative, capturing key details, outcomes, challenges encountered, and lessons learned.

### Process:

1. Completion of Activity: Once an institutional activity, such as an event, workshop, seminar, or any other initiative, reaches its conclusion, the coordinators overseeing the activity are tasked with compiling a detailed report encompassing all pertinent information.

2. Report Compilation: The coordinators meticulously compile the report, detailing various aspects of the activity, including its objectives, participants, agenda, proceedings, notable highlights, achievements, feedback received, and any notable challenges faced during implementation.

3. Approval by the Principal: Upon compilation, the report undergoes scrutiny and approval by the principal or designated authority. This ensures that the report accurately reflects the institution's activities and aligns with its objectives and standards.

4. Submission to the Webmaster: Following approval, the coordinators submit the finalized report to the webmaster. This report serves as a valuable source of information for updating the institution's website and documenting its achievements and ongoing initiatives.

**Active Webmaster Engagement:** The webmaster will maintain active engagement to highlight institutional achievements, events, and updates through the website. Keeping the web content up-to-date and relevant is essential for showcasing the institution's dynamism and fostering stakeholder engagement.

**Conclusion:** These guidelines ensure that the institution's website remains a reliable source of information and a valuable communication tool for all stakeholders. By adhering to these principles, we uphold the integrity, accessibility, and functionality of our online presence, fostering transparency, engagement, and collaboration within the institution and beyond.

## 9. Incident Response and Reporting Policy:

**Introduction:** The Incident Response and Reporting Policy outlines the procedures for identifying, assessing, and responding to security incidents within the institution. The policy aims to ensure swift and effective action to mitigate risks, minimize impact, and maintain the integrity and confidentiality of institutional data and systems.

**Scope:** This policy applies to all faculty, staff, students, contractors, and any other individuals affiliated with the institution who have access to institutional resources or information systems.

### Incident Reporting:

1. Immediate Reporting: Any individual who becomes aware of a security incident, data breach, or any suspicious activity involving institutional resources or information systems must report it immediately to the Administrator.

2. Reporting Channels: Incidents can be reported through designated channels, including email, phone, or in-person communication, to ensure prompt attention and action.

3. Detailed Information: When reporting an incident, individuals must provide detailed information, including the nature of the incident, time and location, individuals involved, and any relevant evidence or documentation.

### Incident Response Process:

1. Initial Assessment: Upon receiving a report of an incident, the Administrator will conduct an initial assessment to determine the severity and scope of the incident.

2. Investigation: If the incident can be resolved at the Administrator level, they will initiate an investigation to gather additional information and assess the impact. If necessary, they may involve relevant personnel or departments to assist in the investigation.

3. Mitigation: The Administrator will take immediate steps to mitigate the incident's impact and prevent further damage or unauthorized access to institutional resources.

4. Notification: If the incident cannot be resolved at the Administrator level, or if it involves significant risks or breaches, the Administrator will promptly notify the Principal/Deans and other relevant authorities.

5. Collaboration: The Administrator will collaborate with relevant stakeholders, such as IT security personnel, legal counsel, and external authorities, as necessary, to address the incident effectively.

6. Documentation: All incidents, investigations, and responses will be thoroughly documented, including actions taken, findings, and recommendations for future prevention.

**Incident Resolution:**

1. Timely Resolution: Every effort will be made to resolve incidents in a timely manner to minimize disruption to institutional operations and prevent further impact.

2. Communication: Throughout the incident response process, clear and timely communication will be maintained with affected parties, stakeholders, and institutional leadership to provide updates on the situation and any remedial actions taken.

**Incident Review and Analysis:**

1. After the resolution of an incident, a post-incident review and analysis will be conducted to assess the effectiveness of the response process, identify any gaps or areas for improvement, and implement corrective measures to prevent future incidents.

2. Lessons Learned: Insights gained from incident reviews will be used to enhance incident response procedures, update security protocols, and provide training and awareness programs to strengthen institutional security posture.

Compliance: All individuals are required to comply with this Incident Response and Reporting Policy. Failure to report security incidents or comply with incident response procedures may result in disciplinary action, including but not limited to reprimand, suspension, or termination of access or employment.

**Conclusion:** The Incident Response and Reporting Policy underscores the institution's commitment to safeguarding its resources, data, and reputation against security threats and breaches. By establishing clear procedures for incident detection, reporting, response, and review, the institution can effectively mitigate risks, minimize impact, and maintain a secure environment for all stakeholders.

## 10. Data Security Policy:

**Introduction:** The Data Security Policy outlines the guidelines and procedures for protecting institutional data from unauthorized access, disclosure, alteration, or loss. The policy aims to safeguard the confidentiality, integrity, and availability of institutional data, ensuring compliance with relevant regulations and standards.

Scope: This policy applies to all faculty, staff, students, contractors, and any other individuals affiliated with the institution who have access to institutional data or information systems.

### Confidentiality of Institutional Data:

1. Non-Disclosure: Institutional confidential data, including sensitive information, proprietary data, and personally identifiable information (PII), shall not be shared with anyone unless authorized by the relevant authorities.

2. Confidentiality Agreement: Individuals with access to institutional data shall be required to sign a confidentiality agreement acknowledging their responsibility to maintain the confidentiality of such data and refrain from unauthorized disclosure or use.

### Ownership of Academic Documents/Data:

1. Institutional Property: All academic documents, data, and intellectual property generated or acquired by employees in the course of their employment are the exclusive property of the institution.

2. Ownership Rights: Employees cannot claim ownership of institutional data or documents, and any attempt to do so is prohibited. This includes research data, course materials, scholarly publications, and other academic works created during their tenure.

### Integrity and Manipulation of Institutional Data:

1. Data Integrity: Institutional data should not be altered, manipulated, or falsified without proper authorization from the concerned authorities.

2. Permission Requirement: Any modifications or changes to institutional data must be approved by the relevant department heads, administrators, or data custodians responsible for managing the data.

### Data Access and Permissions:

1. Need-to-Know Basis: Access to institutional data shall be granted on a need-to-know basis, with permissions assigned according to job roles, responsibilities, and specific data requirements.

2. Access Controls: Access to sensitive or confidential data shall be restricted through user authentication, role-based access controls, encryption, and other security measures to prevent unauthorized access.

### Data Handling and Storage:

1. Secure Storage: Institutional data shall be stored in secure locations, such as password-protected servers, databases, or encrypted storage devices, to prevent unauthorized access or theft.

2. Encryption: Confidential data transmitted over networks or stored on portable devices shall be encrypted to protect against interception or unauthorized disclosure.

### Data Retention and Disposal:

1. Retention Period: Institutional data shall be retained for the period specified in the institution's records retention policy or as required by applicable laws and regulations.

2. Secure Disposal: When data reaches the end of its retention period or is no longer needed, it shall be securely disposed of using approved methods, such as shredding, data wiping, or secure deletion, to prevent unauthorized recovery.

Compliance: All individuals are required to comply with this Data Security Policy and adhere to its guidelines and procedures. Failure to comply may result in disciplinary action, including but not limited to reprimand, suspension, or termination of access or employment.

**Conclusion:** The Data Security Policy underscores the institution's commitment to safeguarding its data assets and ensuring their confidentiality, integrity, and availability. By implementing robust security measures, access controls, and data handling practices, the institution can mitigate risks and protect sensitive information from unauthorized access or misuse.

## 11. Acceptable Use Policy (AUP):

**Introduction:** The Acceptable Use Policy (AUP) outlines the guidelines and rules governing the appropriate use of institutional IT resources and facilities. The policy aims to ensure responsible, ethical, and lawful use of technology resources while promoting a safe and productive computing environment for all users.

**Scope:** This policy applies to all faculty, staff, students, contractors, guests, and any other individuals granted access to institutional IT resources or facilities.

### Acceptable Use:

1. Compliance with Laws and Policies: Users must comply with all applicable laws, regulations, and institutional policies governing the use of IT resources, including but not limited to copyright laws, data protection regulations, and network usage policies.

2. Respect for Others: Users shall respect the rights and privacy of others and refrain from engaging in activities that may cause harm, harassment, or disruption to individuals or groups.

3. Ethical Conduct: Users must uphold ethical standards and refrain from engaging in activities that are fraudulent, deceptive, or malicious, including but not limited to hacking, phishing, or spreading malware.

4. Intellectual Property: Users shall respect intellectual property rights and refrain from unauthorized copying, distribution, or use of copyrighted materials, software, or proprietary information.

5. Network Security: Users are responsible for maintaining the security of their accounts and devices and must not engage in activities that compromise the security or integrity of institutional networks, systems, or data.

6. Resource Conservation: Users shall utilize IT resources responsibly and avoid activities that result in excessive consumption of network bandwidth, storage capacity, or computing resources.

7. Personal Use: Personal use of institutional IT resources is permitted on a limited basis, provided it does not interfere with job duties, violate institutional policies, or consume excessive resources.

8. Prohibited Activities: The following activities are strictly prohibited and constitute a violation of the AUP: a. Unauthorized access to IT resources or accounts. b. Distribution of offensive, discriminatory, or inappropriate content. c. Use of IT resources for illegal or unethical purposes. d. Disruption or interference with network operations or services. e. Violation of software licensing agreements or copyright laws. f. Use of IT resources for personal financial gain or commercial activities without proper authorization.

9. Reporting Violations: Users who become aware of any violations of the AUP are encouraged to report them to the IT department or designated authorities for investigation and appropriate action.

10. Consequences of Violations: Violations of the AUP may result in disciplinary action, including but not limited to suspension or termination of IT privileges, academic sanctions, or legal consequences, depending on the severity of the violation and applicable institutional policies.

**Conclusion:** The Acceptable Use Policy (AUP) serves as a guide for promoting responsible, ethical, and lawful use of institutional IT resources. By adhering to the guidelines outlined in this policy, users can contribute to a safe, secure, and productive computing environment for all members of the institution.

## 12. Software Development and Change Management Policy:

**Introduction:** The Software Development and Change Management Policy governs the development, maintenance, and modification of institutional software systems, including the Information Management System (MIS). This policy ensures the orderly development, testing, and implementation of software changes while maintaining the integrity and security of institutional data.

**Scope:** This policy applies to all software development activities, including the creation, modification, and maintenance of institutional software systems, as well as the implementation of software changes and updates.

## Software Developer Responsibilities:

1. System Integrity: The software developer, acting as the software administrator, is responsible for maintaining the integrity, security, and functionality of the institutional Information Management System (MIS).

2. Development and Maintenance: The software developer is responsible for the ongoing development, enhancement, and maintenance of the MIS software, ensuring that it meets the evolving needs of the institution.

3. Change Management: The software developer shall manage all software change requests, including the evaluation, prioritization, development, testing, and implementation of requested changes.

4. User Education: The software developer shall provide training and education to users on new features, functionalities, or changes implemented in the MIS software, ensuring effective utilization by faculty and staff members.

5. Access Control: The software developer shall maintain strict access controls over the MIS software, ensuring that only authorized personnel have access to sensitive data and system functionalities.

6. Compliance: The software developer shall ensure compliance with relevant regulations, standards, and institutional policies governing software development, data privacy, and security.

## Software Change Management Process:

1. Request Submission: Faculty members shall submit software change requests for the MIS system through the department head, deans, or principal, detailing the specific requirements or modifications needed.

2. Evaluation and Prioritization: The software developer shall evaluate and prioritize change requests based on their impact, urgency, and alignment with institutional objectives.

3. Development and Testing: Approved change requests shall undergo development, testing, and quality assurance processes to ensure the accuracy, reliability, and functionality of the proposed changes.

4. Implementation: Upon successful testing, approved changes shall be implemented into the MIS software system in a controlled manner to minimize disruption and ensure seamless integration.

5. Documentation: The software developer shall maintain comprehensive documentation of all software changes, including change requests, development activities, testing results, and implementation details.

### Webmaster Responsibilities:

1. Web Application Management: The webmaster is responsible for the development, maintenance, and management of all institutional web applications, including the institutional website and related web-based services.

2. Integration: The webmaster shall ensure seamless integration between the MIS software system and institutional web applications, facilitating efficient data exchange and access for users.

3. User Support: The webmaster shall provide technical support and assistance to users of institutional web applications, addressing any issues or concerns related to accessibility, usability, or functionality.

### Faculty Member Responsibilities:

1. Effective Utilization: Faculty members shall utilize the MIS software effectively to manage institutional academic and administrative data, including student records, course information, and other relevant data sets.

2. Collaboration: Faculty members shall collaborate with the software developer and webmaster to provide feedback, suggestions, and requirements for improving institutional software systems and web applications.

**Conclusion:** The Software Development and Change Management Policy ensures the effective development, maintenance, and modification of institutional software systems, including the MIS software, while promoting collaboration, transparency, and compliance with institutional objectives and standards. By adhering to this policy, the institution can leverage technology to enhance operational efficiency, data management, and academic excellence.

## 13. Social Engineering and Phishing Awareness Policy:

**Introduction:** The Social Engineering and Phishing Awareness Policy aims to educate and inform all faculty, staff, students, and contractors about the risks associated with social engineering attacks and phishing attempts. This policy outlines guidelines and best practices to help prevent and mitigate the impact of such attacks on institutional information security.

**Scope:** This policy applies to all individuals who have access to institutional IT resources, including but not limited to computers, networks, email accounts, and online systems.

## Awareness Training:

1. Mandatory Training: All faculty, staff, students, and contractors must undergo mandatory training on social engineering and phishing awareness upon joining the institution. Refresher training shall be provided annually or as necessary to reinforce awareness.

2. Content: Training sessions shall cover topics such as identifying phishing emails, recognizing social engineering tactics, understanding the risks of sharing sensitive information, and reporting suspicious activities to the IT department.

3. Training Delivery: Awareness training sessions may be conducted through online modules, workshops, seminars, or other suitable formats to reach all members of the institution effectively.

## Identification of Social Engineering Attacks:

1. Email Phishing: Users must be vigilant when receiving unsolicited emails requesting sensitive information, login credentials, or financial transactions. Suspicious emails may contain spelling or grammar errors, urgent requests for action, or unfamiliar senders.

2. Phone Calls: Employees should exercise caution when receiving unexpected phone calls requesting personal or confidential information. They should verify the identity of the caller and avoid disclosing sensitive information over the phone.

3. Impersonation: Users should be aware of attempts by malicious actors to impersonate trusted individuals or authority figures to gain access to sensitive information or resources.

## Response and Reporting:

1. Reporting Procedures: All suspected social engineering attacks or phishing attempts must be reported immediately to the IT department or designated authorities for investigation.

2. Incident Response: The IT department shall investigate reported incidents, assess the severity of the threat, and take appropriate actions to mitigate the impact, such as blocking malicious email addresses, updating security controls, or providing additional training to users.

3. Incident Documentation: Details of social engineering incidents, including the nature of the attack, affected users, and response actions taken, shall be documented for future reference and analysis.

## Preventive Measures:

1. Security Awareness: Regular reminders and updates on social engineering and phishing awareness shall be disseminated through internal communications channels, such as newsletters, posters, or email bulletins.

2. Technical Controls: The institution shall implement technical measures, such as email filtering, spam detection, and antivirus software, to detect and block phishing emails and malicious attachments.

3. Multi-Factor Authentication: Multi-factor authentication (MFA) shall be enforced for accessing sensitive systems or applications to provide an additional layer of security against unauthorized access.

4. Education and Training: Ongoing education and training programs shall be provided to empower users with the knowledge and skills to recognize and respond to social engineering attacks effectively.

### Compliance and Enforcement:

1. Non-Compliance: Failure to comply with this policy, including neglecting to report suspected social engineering incidents or disregarding security awareness training, may result in disciplinary action, including but not limited to retraining, suspension of IT privileges, or termination of employment or academic enrollment.

2. Review and Update: This policy shall be reviewed periodically to ensure its effectiveness and relevance to evolving threats and technology trends. Updates or revisions shall be made as necessary to address emerging risks or changes in institutional requirements.

**Conclusion:** The Social Engineering and Phishing Awareness Policy underscores the importance of user education, vigilance, and collaboration in combating social engineering attacks and phishing threats. By raising awareness, implementing preventive measures, and fostering a culture of security consciousness, the institution can better protect its information assets and maintain a secure computing environment for all stakeholders.

## 14. Compliance and Regulatory Policy:

**Introduction:** The Compliance and Regulatory Policy outlines the institution's commitment to adhering to relevant laws, regulations, standards, and industry best practices governing information security, data privacy, and IT operations. This policy aims to ensure legal and regulatory compliance while protecting institutional assets and stakeholders' interests.

**Scope:** This policy applies to all faculty, staff, students, contractors, and any other individuals involved in the use, management, or maintenance of institutional IT resources, data, and systems.

### Legal and Regulatory Compliance:

1. Applicable Laws: The institution shall comply with all applicable laws, regulations, and statutory requirements related to information security, data protection, privacy, intellectual property, accessibility, and other relevant areas.

2. Industry Standards: Where applicable, the institution shall adhere to recognized industry standards, frameworks, and guidelines, such as ISO/IEC 27001, NIST Cybersecurity Framework, GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and FERPA (Family Educational Rights and Privacy Act).

## Data Protection and Privacy:

1. Data Classification: Institutional data shall be classified based on its sensitivity, confidentiality, and regulatory requirements, and appropriate safeguards shall be implemented to protect data integrity and privacy.

2. Consent and Authorization: The institution shall obtain consent and authorization from individuals before collecting, processing, or sharing their personal information, in compliance with applicable data protection laws and regulations.

3. Data Retention: Institutional data shall be retained and disposed of in accordance with established retention schedules, legal requirements, and privacy principles, to minimize the risk of unauthorized access, disclosure, or misuse.

## Intellectual Property and Copyright:

1. Respect for Intellectual Property: The institution shall respect intellectual property rights and comply with copyright laws and licensing agreements when using, reproducing, or distributing copyrighted materials, including software, publications, multimedia content, and academic works.

2. Ownership of Institutional Assets: All intellectual property, including software, research findings, academic publications, and institutional trademarks, developed or produced using institutional resources, shall be owned by the institution, unless otherwise agreed upon in writing.

## Compliance Reporting and Monitoring:

1. Compliance Oversight: The institution shall designate responsible individuals or committees to oversee compliance with applicable laws, regulations, and policies, and ensure that adequate controls are in place to mitigate compliance risks.

2. Monitoring and Auditing: Regular monitoring, auditing, and assessment activities shall be conducted to evaluate compliance with legal, regulatory, and policy requirements, identify gaps or deficiencies, and implement corrective actions as necessary.

3. Reporting Obligations: Any suspected violations of compliance requirements, including breaches of data privacy, security incidents, or regulatory non-compliance, shall be promptly reported to the appropriate authorities, such as the IT department, compliance officer, or regulatory agencies, in accordance with established procedures.

## Training and Awareness:

1. Training Programs: The institution shall provide training and awareness programs to educate faculty, staff, and students about their obligations and responsibilities regarding compliance with relevant laws, regulations, and institutional policies.

2. Role-Specific Training: Training initiatives shall be tailored to address the specific compliance requirements and responsibilities of different roles and functions within the institution, ensuring that individuals understand their role in maintaining compliance.

## Enforcement and Consequences:

1. Compliance Violations: Non-compliance with this policy, applicable laws, regulations, or institutional policies may result in disciplinary action, including but not limited to retraining, suspension of privileges, termination of employment, academic sanctions, or legal consequences, as determined by institutional policies and procedures.

2. Reporting Non-Compliance: Individuals who become aware of actual or potential compliance violations shall promptly report such incidents to the appropriate authorities for investigation and resolution.

**Conclusion:** The Compliance and Regulatory Policy underscores the institution's commitment to upholding legal and regulatory requirements, protecting data privacy and intellectual property, and fostering a culture of compliance across the organization. By adhering to this policy. and related procedures, the institution can mitigate compliance risks, safeguard institutional assets, and maintain trust and credibility with stakeholders and regulatory authorities.