Shri Guru Gobind Singhji Institute of Engineering and Technology

Vishnupuri, Nanded (Maharashtra State) INDIA PIN 431606
Government Aided Autonomous Institute DTE Code: 2020
NAAC Accredited institute GRADE B++, CGPA 2.91 (2020 -2025)
Vision Statement: Education of Human Power for Technological Excellence

(An Autonomous Institute of Government of Maharashtra)

Information Technology Policy

Institute Vision and Mission

VISION

"Education Of Human Power for Technological Excellence"

MISSION

- Dissemination of knowledge by offering world-class education
- Right to information for all stakeholders
- Promotion of sustainable industrialization to development of appropriate technologies
- Continuing education programs for re-engineering of regional socio-economic system in the light of dynamic, global technological changes
- Contribution to national wealth through innovation

September -2024

Contents:

1.Preamble:

At Shri Guru Gobind Singhji Institute of Engineering and Technology (SGGS IE&T), we recognize the critical importance of effectively managing Software and hardware resources to support our academic, research, and administrative activities.

This policy outlines the guidelines and procedures for managing, acquiring, deploying, and maintaining Software and hardware resources within the Institute.

In pursuit of academic excellence, technological innovation, and the advancement of knowledge, SGGS IE&T is dedicated to fostering a robust Information Technology (IT) ecosystem. Our IT Policy serves as a guiding beacon, delineating the principles, practices, and protocols governing the institution's strategic management and utilization of IT resources.

Recognizing the pivotal role of Information Technology in shaping the educational landscape, research endeavors, and administrative functions, SGGS IE&T reaffirms its commitment to harnessing the transformative power of IT to drive progress and achieve our institutional objectives.

2.Objectives:

Through this policy, we articulate our unwavering dedication to:

1. Providing state-of-the-art IT infrastructure: SGGS IE&T acknowledges the fundamental importance of robust Hardware, Software, networking, and digital services in facilitating teaching, learning, research, and administrative functions. We are committed to providing cutting-edge technologies and infrastructure to create an environment conducive to innovation and collaboration.

2. Ensuring cybersecurity and data protection: SGGS IE&T prioritizes the security and integrity of digital assets, intellectual property, and sensitive information. We are steadfast in our commitment to implementing robust cybersecurity measures, fostering stakeholder awareness, and adhering to best practices to safeguard against cyber threats and vulnerabilities.

3. Promoting accessibility and inclusivity: SGGS IE&T is dedicated to ensuring that all members of our academic community have equitable Access to IT resources, services, and support. We strive to create an inclusive environment where diversity is celebrated, and individuals of all backgrounds can leverage technology to pursue their academic and professional aspirations.

4. Fostering innovation and digital literacy: SGGS IE&T recognizes the transformative potential of Information Technology in driving innovation and fostering digital literacy. We are committed to providing experimentation, exploration, and learning opportunities in emerging technologies, empowering our students, faculty, and staff to thrive in the digital age.

5. Upholding ethical standards and regulatory compliance: SGGS IE&T places utmost importance on integrity, ethics, and compliance with regulatory requirements in all IT-related activities. We are committed to promoting responsible conduct, transparency, and accountability in the use of IT resources and adherence to relevant laws and regulations.

6. Paperless Office and Cashless system: SGGS IE&T promotes and implements paperless Office by minimal paper-based processes and relies on digitized documents instead. This is inspired by the Digital India initiative launched by the Government of India. It's safe to say that cashless transactions have revolutionized India's financial outlook. The convenience and security associated with these payment modes are essential to the surge. With the recent introduction of several digital modes of payment in India, we are slowly adapting to the shift. In cashless transactions, payments are made or accepted without hard cash. This includes payments made via credit/debit cards, cheques, DD, NEFT, RTGS, or any other form of online payment that removes the need for cash.

7. Use and promote open source software (OSS): SGGSIE&T created an institute-wide policy to ensure all stakeholders are informed to use open source software (especially in products). This will help maximize the impact and benefit of using open source and ensure that any technical, legal, or business risks are adequately mitigated. One more Objective is to provide strategic control in applications and systems from a long-term perspective and reduce projects' Total Cost of Ownership (TCO).

Through steadfastly implementing this IT Policy, SGGS IE&T reaffirms its commitment to excellence, integrity, and continuous improvement in leveraging Information Technology to enhance teaching, learning, research, and administrative functions. Together, we strive to position SGGS IE&T as a leading institution at the forefront of technological innovation and academic excellence.
The policies in this document are official policies sponsored by or endorsed by the SGGS IE&T IE&T Nanded.

3. Information Technology (IT) Policy

The following committees are working to ensure the Institute's smooth implementation of IT policy.

Institute Information Technology Committee (IITC)

1	Director, SGGS IE&T IE& T	Chairman
2	Head of All the Departments	Members
3	Dean, Procurement	Member
4	Dean Finance,	Member
5	Dean IT Services	Member Secretary

IITC is responsible for the following activities:

1. Requirement analysis of the IT infrastructure (Hardware, software, software or cloud services subscriptions) in the Institute
2. Propose and revise the Institute's IT policies.
3. Handle IT policy violation cases, if any.
4. Prepare and submit a budget for requirements of IT infrastructure such as Hardware, Software, Annual Maintenance Contracts (AMC), software/hardware subscriptions, etc., at the Institute to the Dean of Finance before February every year.
5. Evaluate the proposals submitted by the DITC for Hardware, Software, Annual Maintenance Contracts (AMC), Software subscriptions, etc, for the departments and submit them to the Dean of finance.

Departmental Information Technology Committee (DITC)

1	Head of the Department	Chairman
2	Faculty Members (Two Lab In-charge)	Members
3	IT-Coordinator (Lab In-charge)	Member Secretary

DITC is responsible for the following activities:

1. Requirement analysis of the Department's IT infra.
2. Observe IT policy implementation in the Department.
3. Report to the IITC for any IT policy violations.
4. Prepare and submit a budget for the Department for IT infrastructure requirements such as hardware, software, annual maintenance contracts (AMC), software/hardware subscriptions, etc.
5. Evaluate the departmental IT infrastructure occasionally and submit the report to the IITC.
6. Generate or raise any service request to get support for IT infrastructure-related issues.

IT Services Section

1	Dean	Overall coordination, procurement monitoring, and management of IT services on campus.
2	Campus Networking Unit	Monitoring and management of networking infrastructure on the campus.
3	Website Management Unit	Development, Update, and maintenance of networking infrastructure on the campus.
4	Support and Maintenance Section	Institute Hardware, Software, licensing, AMC, and renewals of products.
5	ERP Unit	Requirements gathering, procurement customization, Update, and maintenance of ERP.
6	Central Computing Facility (CCF) Unit	Providing Computing facilities at the Institute level.

Responsibilities of Dean IT Services:

The IT services section is the backbone of an organization's technological foundation. Members in this Section are the silent heroes who ensure everything runs smoothly behind the scenes. Here's a breakdown of the key roles and responsibilities of the Dean of IT services:

Maintaining the Infrastructure:

- **Hardware and Software Management:** Install, configure, and maintain computer systems, networks, printers, and other equipment. This ensures everything is functioning correctly and up to date.
- **System Monitoring:** Proactively monitor systems and networks for any glitches or potential problems. This helps prevent downtime and ensures smooth operations.

Supporting the Users:

- **Help Desk:** IT services typically house the help desk, which is the first point of contact for users facing technical issues. Troubleshoot problems, reset passwords and provide technical support via various channels.
- **User Accounts and Access:** Set up new user accounts, manage access permissions to various systems and data, and ensure data security.

Other Key Responsibilities:

- **Security:** IT services are vital in safeguarding the organization's IT infrastructure from cyber threats. This involves implementing firewalls, antivirus software, and other security measures.
- **Communication and Collaboration Systems:** Manage critical applications like email, web-server, portals, Video Surveillance, and video conferencing, ensuring availability and security.
- **Staying Updated:** The IT field constantly evolves, so IT services professionals must stay updated on the latest technologies and trends to support the organization's needs best.

The IT services section keeps the organization's technological house in order. Ensure support staff have the tools they need to function effectively and securely while safeguarding the organization's data and systems.

Defined Policies:

The Institute's central Information Technology Services (IT) Policy consists of the following policies.

1. IT Hardware Policy
2. Software Policy

3. Network(Internet/Intranet) Policy
4. Email Account Policy
5. Social Media Policy
6. Information Security Policy
7. Video Surveillance Policy
8. IT infrastructure (hardware/software/network/web) Support Policy
9. Institute Enterprise Resource Planning (ERP) Policy
10. Institute Web site policy

Violations and Penalties:

Policy violations may result in disciplinary action, including dismissal from employment, expulsion from further study and termination, or suspension of network privileges. Detailed guidelines are defined in Appendix –A

3.1 IT Hardware Policy

The institute network user community needs to observe certain precautions while getting their computers or peripherals installed so that they may face minimum inconvenience due to the interruption of services due to hardware failures.

Hardware policy defines the following terms:

- Primary User - Device used by a single user and by the Department
- End User System – Device used by individuals and by the Department.

3.1.1 Warranty & Annual Maintenance Contract

Computers purchased by any Section/Department/Project should preferably have a 3-year on-site comprehensive warranty.

3.1.2 Power Connection to Computers and Peripherals

All the computers and peripherals, including networking devices, should be connected to the electrical point strictly through UPS.

3.1.3 Network Cable Connection

While connecting the computer to the Network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with network communication.

3.1.4 File and Print-Sharing Facilities

When shared through the Network, files should be protected with a password and read-only access rule.

3.1.5 Maintenance / Support of Hardware Issues

- DITC will raise support tickets to seek hardware-related help and maintenance, if any, in the Department.
- All other individual users using the Institute's IT infrastructure may create the support ticket by using the support system available on the Website.

Guidelines are defined in **Appendix -B**.

3.2 Software Policy

Any computer or hardware purchases made by the individual departments/projects should address the following points.

- Ensure that computer systems or Hardware have all licensed software (operating system and necessary application software) installed.
- Institute IT policy does not allow pirated/unauthorized software installation on the Institute-owned computers and the computers connected to the Institute campus network.
- Promote the use of open-source Software in the Department.
- The DITC must approve the requirement for Software in the Department.
- The Software to be purchased should be required for the concerned Department only.
- If pirated/ unlicensed Software is installed by an individual or by the Department, It will be the sole responsibility of the individual/Department for the consequences arising out of it. If the Institute is penalized due to a student's violation of this policy, then the student will be liable for the same.

3.2.1 Campus Networking Unit /Central Computing Facility Interface

- The Campus Networking Section, upon finding a non-compliant computer, will notify the individual responsible for the system and ask that it be brought into compliance.
- Notification will be sent via email/telephone, and a copy of the notification will be sent to the CCF if applicable.
- The individual user will follow up on the notification to ensure their computer gains necessary compliance. The Campus Networking section will guide as needed for the individual to gain compliance.

3.2.2 Software-related issues

- DITC will raise support tickets to seek software-related help and maintenance, if any, in the Department.
- All other users using the Institute's IT infrastructure may create a support ticket using the support system available on the Website.

3.3. Network (Intranet & Internet) Policy

- Network connectivity is provided either through an authenticated network access connection or a Virtual Local Network **(VLAN**) connection.

- It is governed under the Institute IT Policy.

- The Campus Networking is responsible for the ongoing maintenance and support of the Network, exclusive of local applications.

- Problems within the Institute's Network should be reported to Campus Networking Unit

3.3.1 IP Address Allocation

- Any computer (PC/Server) that will be connected to the Institute network will have an IP address assigned by the Campus Networking Unit following a systematic approach.
- As and when a new computer is installed in any location, the concerned device will get the IP address from the Campus Networking Unit automatically.

3.3.2 DHCP and Proxy Configuration by Individual Departments /Sections/ Users

- The use of any computer at the end-user location as a DHCP server to connect to more computers through an individual switch/hub and distribute IP addresses (public or private) should be strictly avoided.

- Even the configuration of any computer with an additional network interface card and connecting another computer to it is considered a proxy/DHCP configuration.

- Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the Network.

- The connection will be restored after receiving written compliance assurance from the relevant department/user.

3.3.3 Running Network Services on the Servers

- Individual departments/individuals connecting to the Institute network over the LAN may run server software (e.g., HTTP/Web server, SMTP server, FTP server) only after bringing it to the knowledge of the Campus Networking Unit in writing and after meeting the requirements of the Institute IT policy.

- Non-compliance with this policy is a direct violation of the Institute IT policy and will terminate their connection to the Network.
-
- The Campus Networking Unit takes no responsibility for the content of machines connected to the Network, regardless of whether those machines are Institute or personal property.
-
- The Campus Networking Unit will be constrained to disconnect client machines where potentially damaging Software is found to exist.
-
- A client machine may also be disconnected if the client's activity adversely affects the Network's performance.
-
- Access to remote networks using an Institute's network connection must comply with all policies and rules of those networks. This applies to any networks to which the Institute Network connects. Institute network and computer resources are not used for personal or commercial purposes. Network traffic will be monitored for security and performance reasons at the Campus Networking section.

- The impersonation of an authorized user while connecting to the Network is a direct violation of this agreement and will result in the termination of the connection.
  Guidelines are defined in **Appendix -C.**

3.4. Email Account Policy

- To increase the efficient distribution of critical information to all faculty, staff and students, and the Institute's administrators, utilizing the Institute's email services for formal Institute communication and academic & other official purposes is recommended.

- The email address must be kept active and used regularly to receive these notices. Staff and faculty may use the email facility by logging in with their User ID and password.

- The IT service section creates the Institute's email accounts; modification requests for email accounts and passwords can be made by applying.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

1. The facility should be used primarily for academic and official purposes and to a limited extent, for personal purposes.

2. Using the facility for illegal/commercial purposes is a direct violation of the Institute's IT policy and may entail withdrawal of the facility.

3. The user should take care of any mail or attachments from unknown and suspicious sources while opening them, even if they are from a known source and contain any suspicious or suspicious attachments.

4. Users should configure messaging software on the computer they use permanently to download the mail in the mailbox onto their computer periodically.

5. Users should refrain from intercepting or trying to break into others' email accounts, as it is infringing the privacy of other users. This act is liable for punishment under IT Act.

6. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user and should be promptly closed.

7. Impersonating the email accounts of others will be taken as a severe offense under the Institute IT security policy.

11. It is ultimately everyone's responsibility to keep their email account accessible from violations of the Institute's email usage policy.

12. Email ID provided by the Institute is valid for Lifetime unless used for only personal purpose.

13. Student users will get cloud storage space up to 50 GB for four years and 15 GB after pass-out for a Lifetime. This is also applicable to the retried faculty as well. Regular faculty on roll/Institute Clubs get 100 GB storage.
14. For extra storage requests should be forwarded with justification and approval from the concerned authority

The above laid down policies are broadly applicable even to the email services that are provided by other sources such as Gmail.com, etc., as long as they are being used from the Institute's campus network or by using the resources provided by the Institute to the individual for official use even from outside.
Guidelines are defined in **Appendix -D**.

3.5. Social Media Policy

This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include

- What's App,
- message boards,
- chat rooms,
- electronic newsletters,
- online forums,
- social networking sites,
- and other sites and services that permit users to share information with others.

PROCEDURES

The following principles apply to professional use of social media on behalf of SGGS IE&T and personal use of social media when referencing SGGS IE&T IE & T.

- When using social media about SGGS IE&T Institute, employees need to know and adhere.

- Employees should be aware of the effect of their actions on their images, as well as SGGS IE&T Institute's Image. Employees post or publish information that may be public information for a long time.
-
- Employees should be aware that The Institute may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to SGGS IE&T, its employees, or stakeholders.
-
- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment or which may hurt religious & Sentiments of anyone or any Community. This is strictly prohibited and liable for punishment under the IT Act.
-
- Employees are not allowed to publish, post, or release any information considered confidential or not public. Employees should check with the EST if there are questions about what is considered confidential.
-
- Social media networks, blogs, and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to the authorized Institute spokespersons.
-
- If employees encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of EST.
-
- Employees should get appropriate permission before they refer to or post images of current or former employees, members, vendors, or suppliers. Additionally, employees should get

permission to use a third party's copyrights, copyrighted material, trademarks, service marks, or other intellectual property.

-
- Social media use shouldn't interfere with employees' responsibilities at SGGS IE&T.
-
- The Institute's computer systems are only for academic and official purposes. When using the Institute's computer systems, use of social media for business purposes is allowed only to those staff whose work profile requires the use of social media (ex, Facebook, Twitter, SGGS IE&T blogs, and LinkedIn, WhatsApp, Instagram, any other), but personal use of social media networks or personal blogging of online content during office hours is discouraged and could result in disciplinary action.
-
- Subject to applicable law, after-hours online activity that violates any other Institute's policy may subject an employee to disciplinary action.
-
- Employees should keep SGGS IE&T-related social media accounts separate from personal accounts.
-
- Employees should not use offensive /abusive language or comment/post any photo that is not in line with their image as a faculty/Teacher (As they belong to a very respected community).

3.6. Information Security Policy

3.6.1 Institute Policy

SGGS IE&T appropriately secures its information from unauthorized access, loss, or damage while supporting our academic culture's open information-sharing needs.

3.6.2. Restricted Information

The following Institute Information is classified as Restricted:

- Bank account number
- Employees Personal details (AADHAR, PAN etc)
- Protected health information

I. State and central laws require that unauthorized access to certain restricted information be reported to the appropriate agency or agencies.

II. All reporting of this nature to external parties must be done by or in consultation with the Office of the Institute Information Officer or Registrar.

III. Sharing Restricted information within the Institute may be permissible if necessary to meet the Institute's legitimate business needs. Except as otherwise required by law (or for purposes of sharing between law enforcement entities), no Restricted information may be disclosed to parties outside the Institute, including contractors, without the proposed recipient's prior written agreement.

IV. (a) to take appropriate measures to safeguard the confidentiality of the Restricted information.

V. (b) not to disclose the Restricted information to any other party for any purpose absent the Institute's prior written consent or a valid court order or subpoena; and

VI. (c) to notify the Institute in advance of any disclosure under a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this policy.

VII. Any restricted information sharing within the Institute must comply with Institute policies, including Rights, Rules and Responsibilities, and Acceptable Use Policy for SGGS IE&T Institute Information Technology and Digital Resources.

3.6.3 Confidential Information

Institute Information is classified as Confidential if it falls outside the restricted classification but is not intended to be shared freely within or outside the Institute due to its sensitive nature and contractual or legal obligations.

Examples of Confidential Information include all non-restricted information contained in personnel files, misconduct and law enforcement investigation records, internal financial data, donor records, and education records.

Sharing of Confidential information may be permissible if necessary:

- To meet the Institute's legitimate business needs.
- Unless disclosure is required by law (or for purposes of sharing between law enforcement entities), when disclosing Confidential information to parties outside the Institute, the proposed recipient must agree

(i) to take appropriate measures to safeguard the confidentiality of the information:

(ii) not to disclose the information to any other party for any purpose absent the Institute's prior written consent or a valid court order or subpoena; and

(iii) to notify the Institute before any disclosure under a court order or subpoena unless the order or subpoena explicitly prohibits such notification.

In addition, the proposed recipient must abide by the requirements of this policy. Any sharing of Confidential information within the Institute must comply with Institute policies, including Rights, Rules, and Responsibilities, as well as the Acceptable Use Policy for SGGS IE&T Institute Information Technology.

3.6.4 Unrestricted Within SGGS IE&T (UWS)

Institute Information is classified as Unrestricted Within SGGS IE&T (UWS) if it falls outside the Restricted and Confidential classifications but is not intended to be freely shared outside the Institute. One example is the faculty profile on the Institute's social media page.

3.6.5 Publicly Available

Institute Information is classified as Publicly Available if it is intended to be made available to anyone inside and outside of SGGS IE&T Institute.

3.6.6 Protection, Handling, and Classification of Information

1. Based on its classification, Institute Information must be appropriately protected from unauthorized access, loss, and damage. The SGGS IE&T Information Protection Standards and Procedures contain specific security requirements for each classification.
2. Handling Institute Information from any source other than SGGS IE&T Institute may require compliance with this policy and the requirements of the individual or entity that created, provided, or controls the information. If you have concerns about your ability to comply, consult the relevant senior executive and the Office of the General Counsel.
3. When deemed appropriate, the classification level may be increased, or additional security requirements may be imposed beyond what is required by the Information Security Policy and SGGS IE&T Information Protection Standards and Procedures.
4. If you receive Controlled Unclassified Information (CUI) or create it, contact the Information Security Office (ISO) to ensure appropriate security controls are applied to the data. If you are unsure whether it is CUI, please contact the Office for Research Project Administration or the ISO.

3.6.7 Responsibilities

All SGGS IE&T Institute faculty, staff, students (when acting on behalf of the Institute through service on Institute bodies), and others granted use of Institute Information are expected to:

- Understand the information classification levels defined in the Information Security Policy.
- As appropriate, classify the information for which one is responsible accordingly.
- Access information only as needed to meet legitimate business needs.

- Not divulge, copy, release, sell, loan, alter, or destroy any Institute Information without a valid business purpose and authorization.
- Protect the confidentiality, integrity, and availability of Institute Information in a manner consistent with the information's classification level and type.
- Handle information by the SGGS IE&T Information Protection Standards and Procedures and any other applicable Institute standard or policy.
- Safeguard any physical key, ID card, computer account, or network account that allows one to access Institute Information.
- Discard media containing SGGS IE&T IE&T information in a manner consistent with the information's classification level, type, and any applicable Institute retention requirement. This includes information in any hard copy document (such as a memo or report) or in any electronic, magnetic, or optical storage medium (such as a memory stick, CD, hard disk, magnetic tape, or disk).
- Contact the Office of the Institute Information Officer before disclosing information generated by that Office or before responding to any litigation or law enforcement subpoenas, court orders, and other information requests from private litigants and government agencies.
- Contact the appropriate Institute office before responding to requests for information from regulatory agencies, inspectors, examiners, and auditors.

3.7. Video Surveillance Policy

3.7.1. The system

1.The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.

2. Cameras will be located at strategic points on the campus, principally at the entrance and exit points of sites and buildings. No camera will be hidden from view, and all will be prevented from focusing on private accommodation's frontages or rear areas.

3. Signs will be prominently placed at strategic points and at campus entrance and exit points to inform staff, students, visitors, and public members that a CCTV/IP Camera installation is in use.

4. Although every effort has been made to ensure the system's maximum effectiveness, it is impossible to guarantee that the system will detect every incident within the coverage area.

The Institute has installed the system with the primary purpose of reducing the threat of crime generally, protecting institution premises, and helping to ensure the safety of all staff, students and visitors are consistent with respect for the individual's privacy.

These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension, and prosecution of offenders of crime and public order
- Facilitate the identification of any activities/events which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

- In the case of security staff, provide management information relating to employee compliance with contracts of employment

The system will not be used for:

- To provide recorded images for the worldwide web.
- To record sound other than by the policy on covert recording.
- For any automated decision making

3.7.2 The Security Control Room

1. Images captured by the system will be monitored and recorded in the Security Control Room, "the control room," twenty-four hours a day throughout the year. Monitors are not visible from outside the control room.
2. No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorized members of senior management, police officers, and any other person with statutory powers of entry.

3. Staff, students, and visitors may be granted Access to the Control Room on a case-by-case basis and only then on written authorization from the Registrar. In an emergency and where it is not reasonably practicable to secure prior approval, access may be granted to persons with a legitimate reason to enter the Control Room.

4 Before allowing access to the control room, staff will satisfy themselves with the identity of any visitor and ensure that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitors' log, including details of their name, the Department or organization they represent, the person who granted authorization, and the times of entry to and exit from the center.

A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

3.7.3 Access To Images

1. All Access to images will be recorded in the Access Log as specified in the Procedures Manual
2. Access to images will be restricted to those staff need to have access by the purposes of the system
3. Access to images by third parties
4. Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal inquiry or the prevention of terrorism and disorder

- Prosecution agencies

- Relevant legal representatives

The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime

• People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal inquiries or criminal proceedings.

• Emergency services in connection with the investigation of an accident.

3.8 IT Infrastructure Support or Maintenance Policy

3.8.1. Maintenance of Computer Hardware & Peripherals

- The Department is responsible for raising support tickets for maintenance of the Institute's computer systems and peripherals under warranty or an annual maintenance contract.
- IT infrastructure that is out of warranty and requires maintenance should be repaired with the help of the IT services section.
- Support is available at itsupport@sggs.ac.in

3.8.2. Raising Complaints for Network Issues

- The Department may raise complaints to the IT service section regarding the particular computer systems or network devices causing network-related problems.
- The designated person in the IT services section receives complaints from the users/department of these computer systems or devices and coordinates with the service engineers of the respective brands of the computer systems or devices to resolve the problem within a reasonable time limit.
- All other individual users facing Network related problems can write networkadmin@sggs.ac.in

3.8.3 Raising Complaints for Email Issues

The IT service section creates the Institute's email accounts; modification requests for email accounts and passwords can be made by applying the IT services Section.
Email support is available admin@sggs.ac.in.

3.8.4 Raising Complaints for Websites
Departments or faculty members can contact webadmin@sggs.ac.in for content posting, modification, and removal on the Website.

3.9 Institute ERP Policy

This Enterprise Resource Planning (ERP) System Policy outlines the procedures and guidelines for accessing, using, and maintaining the Institute's ERP system.
This policy aims to ensure the secure, efficient, and responsible use of the ERP system to support Institute operations and decision-making.

3.9.1 User Access and Permissions

- Access to the ERP system will be granted based on the principle of least privilege. Users will only be given access to the modules and data relevant to their specific roles and responsibilities within the Institute.

- In collaboration with department heads, the IT department will determine and assign user access levels and permissions within the ERP system.

- Users are responsible for maintaining the confidentiality of their assigned username and password. Sharing login credentials is strictly prohibited.

3.9.2 Data Security and Privacy

- The Institute is committed to protecting the confidentiality, integrity, and availability of all data stored within the ERP system.

- Security measures include:
- Regular data backups to ensure disaster recovery.
- Encryption of sensitive data at rest and in transit.
- User activity logs to monitor system access and identify potential security breaches.
-
- Users are prohibited from accessing, modifying, or deleting data beyond their authorized access level.
- Any suspected data breaches or security incidents must be reported to the IT department immediately.

3.9.3 Data Entry and Reporting

- Users are responsible for the accuracy and completeness of the data they enter into the ERP system.
- Data entry procedures and validation processes will be established to minimize errors and inconsistencies.
- The IT Services section will provide training on proper data entry and reporting practices for users with data entry responsibilities.
- Users are encouraged to utilize the reporting functionalities within the ERP system to generate reports and analyze data relevant to their work.

3.9.4 System Change Management

- Any proposed changes to the ERP system configuration, functionality, or integrations with other systems must be submitted through a formal change management process.
- The change management process will ensure a thorough evaluation of proposed changes to minimize disruption to ongoing operations and mitigate potential security risks.

3.9.5 User Training and Support

- The IT department will offer training sessions on user navigation and functionalities within the ERP system. Training will be tailored to the specific needs of different user groups.
- User manuals, online resources, and knowledge base articles will be made available to provide ongoing support for users navigating the ERP system.

3.9.6. Non-Compliance

- Violations of this policy, including unauthorized access, data breaches, or misuse of the system, may result in disciplinary action, including suspension or termination of ERP system access privileges.

3.9.7 Review and Updates

- This policy will be reviewed periodically to reflect technological changes, Institute practices, or relevant regulations. Users will be notified of any policy updates.

3.9.8 Contact Information

- For questions regarding the ERP system or this policy, please contact the IT Services section at erp@sggs.ac.in.

- By implementing this ERP Policy, SGGS IE &T can ensure a secure, efficient, and reliable ERP system to support its core administrative functions and inform future decision-making.

3.10 Institute Website Policy

This website policy outlines the terms and conditions governing your use of the SGGS IE & T website (the "Website"). You agree to be bound by these terms and conditions by accessing or using the Website.

3.10.1. Content Accuracy and Disclaimer

SGGS IE & T strives to provide accurate and up-to-date information on the Website. However, the Institute does not warrant the accuracy, completeness, or reliability of the information on the Website. The information is provided for informational purposes only and should not be construed as professional advice. You are encouraged to verify any information with the appropriate authorities at SGGS IE & T.

3.10.2. Use of the Website

The Website is for your personal, non-commercial use. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, or sell any information, Software, products, or services obtained from the Website.

3.10.3. Intellectual Property

The Website's content, including text, graphics, logos, images, and Software, is the property of SGGS IE & T or its licensors and is protected by copyright and other intellectual property laws.

3.10.4. Links to Third-Party Websites

The Website may contain links to third-party websites. These links are provided for your convenience only and do not constitute an endorsement by SGGSIE&T of the content on such websites. SGGS IE & T is not responsible for the content of linked websites.

3.10.5. Privacy Policy

SGGSIE&T is committed to protecting your privacy. Please refer to our separate Privacy Policy for information on how we collect, use, and disclose your personal information. You can find the Privacy Policy link on the Website footer.

3.10.6. Disclaimer of Warranties

The Website is provided "as is" without express or implied warranties. SGGS IE & T disclaims all warranties, including, but not limited to, warranties of merchantability, fitness for a particular purpose, and non-infringement.

3.10.7. Limitation of Liability

SGGS IE & T will not be liable for any damages arising out of or in connection with your use of the Website, including, but not limited to direct, indirect, incidental, consequential, punitive, or special damages.

3.10.8. Governing Law and Jurisdiction

These terms and conditions will be governed by and construed by the laws of GOI without regard to its conflict of law provisions. Any dispute arising out of or relating to these terms and conditions will be subject to the exclusive jurisdiction of the courts located in Maharashtra.

3.10.9. Changes to this Policy

SGGS IE & T reserves the right to change this policy at anytime. We will post any changes on the Website. It is your responsibility to review the Website for updates periodically.

3.9.10. For support

If individuals have any questions about this policy, support is available at webadmin@sggs.ac.in.

Prof. H. P. Ambulgekar	**Dr. A. V. Nandedkar**	**Dr. M. B. Kokare**
Dean Innovation and Incubation Cell	Policy Coordinator	Director
SGGSIE&T, Nanded	SGGSIE&T, Nanded	SGGSIE&T, Nanded

Appendix -A

Guidelines for Compliance

Penalties

All faculty, students, staff, departmental computer users, authorized visitors, and others who may be granted use of the Institute's systems and network services or Institute-contracted services must comply with the Institute's policies.

- When a member of the Institute community is found to violate this policy, disciplinary action is handled by the average Institute authority and via the normal disciplinary process that would apply to other types of infractions.
- The Institute sponsor or host may be held accountable when an authorized visitor or departmental computing account user violates the policy. If the matter involves illegal action, law enforcement agencies may become involved, as they would for campus actions that do not include information technologies or the Internet.

Institutional Use

- As a member of the Institute community, you are provided with scholarly or work-related tools, including (but not confined to) access to the Library and its systems, to specific computer systems, servers, Software, printers, services, databases, and electronic publications; to the campus telephone and unified messaging systems; and the Internet.
- Your use of all information technology should be for purposes that are consistent with the non-profit educational mission and the policies of the Institute and should comply with any applicable license agreement and terms of service. Members of the Institute community are prohibited from using Institute information technology and digital resources for commercial purposes.
- Computing and network equipment and mobile devices purchased by the Institute remain the property of the Institute, even if they are dedicated for your use. Equipment purchased under research or other grants is usually vested with the Institute, though it is to be used for the grant. When institute-owned equipment is no longer needed, its disposition must comply with institute policy, including the information security policy, and may not be determined independently by the equipment user.
- Those purchasing networked devices using Institute funds or credit cards must follow normal Institute purchasing procedures, as for all other Institute purchases.
- Tampering with Institute-owned IT equipment, including cell or smartphones, is defined as making unauthorized changes to the hardware or system-level software that may conflict with licensing agreements or void applicable warranties. Institute employees must not perform or condone such actions. Exceptions may sometimes be made for academic research purposes.

Personal Use

- Personal use of the Institute's IT and digital resources, except for students enrolled at the Institute, should be incidental and minimal.
- Use of such resources by an employee for non-work-related matters should be reasonable and limited so that it does not prevent the employee from attending to and completing work effectively and efficiently, does not incur additional cost to the Institute, and does not preclude others with work-related needs from using the resources, including the shared campus and Internet bandwidth.
- Individual departments or sections may restrict their employees' personal use of the resources.

Accessibility

- Suppose you develop or acquire information technology and/or digital Hardware, Software, or systems for the Institute for use by students, faculty, staff, or the public. In that case, you are strongly encouraged to ensure that the result will be accessible to all individuals, including those with disabilities.
- Suppose a service or system is not accessible at the time of acquisition. In that case, you are strongly encouraged to work with the vendor to ensure that accessibility enhancements will be provided over time and to provide an effective alternative format in the interim.
- Offices seeking information, assistance and training regarding digital accessibility should consult the IT services Section.

The Institute's Right to Access Files

- All information stored on or transmitted through the Institute's electronic services, equipment, and systems, including but not limited to servers, computers, mobile devices, telephone systems, and cloud-hosted services and storage (collectively, "IT Systems") is subject to the rules of SGGS IE&T Institute.
- The Institute has the legal right to access, preserve, and review all information stored or transmitted through its IT Systems.
- Non-intrusive monitoring of campus network traffic occurs routinely to ensure acceptable performance and to identify and resolve problems. If problem traffic patterns suggest that system or network security, integrity, or performance has been compromised, networking and monitoring systems staff will investigate, and protective restrictions may be applied until the condition has been rectified. By attaching privately owned personal computers or other information technology resources to the Institute's Network, users consent to the Institute's use of scanning programs for security purposes on those resources while attached to the Network.
- Some departments that maintain servers or internal networks may collect usage data and monitor such servers or networks to ensure adequate technical performance. Departments that collect such data are expected to protect the privacy of those using the resources.
- The Institute also provides some access to accounts, files, and documents residing on Institute-owned equipment and systems (and transmitted via the Institute's network services) to outside vendors who have been contracted to provide technology services, including email protection services. The Institute's contracts with such vendors contain firm provisions for the security of information and the privacy of members of the Institute community who may use those services.
- To comply with (a) central, state, or local law or rules or (b) validly issued subpoenas, governmental information requests, warrants, court orders, or discovery obligations in a pending or reasonably anticipated legal proceeding, the Institute may be required to access, preserve, review or produce information stored on or transmitted through its IT Systems.
- It is essential to contact the Office of the Registrar before disclosing any information in response to any subpoenas, court orders, or other information requests from litigants or government agencies.

Appendix -B

Hardware Usage Guidelines

1. Maintenance of Computer Hardware & Peripherals
The Department is responsible for maintaining the Institute-owned computer systems and peripherals that are either under warranty or annual maintenance contract and whose responsibility has officially been entrusted to the IT services.

2. Receiving Complaints
The Department may receive complaints from the Campus Networking section if any particular computer systems are causing network-related problems. The Department may receive user complaints if any computer systems or peripherals under maintenance have issues.
The designated person in the Department receives complaints from the users/Campus Networking unit of these computer systems and coordinates with the service engineers of the respective brands of the computer systems to resolve the problem within a reasonable time limit.

3. Scope of Service
The Department will be responsible only for solving Hardware problems or OS or any other application software that was legally purchased by the Institute and was loaded by the company.

4. Reporting IT Policy Violation Incidents
Suppose the Department or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the Institute. In that case, such incidents should be brought to the notice of the Campus Networking Unit and Institute authorities.

5. Reporting incidents related to Network Operations
When the network port of any particular computer system is turned off due to a virus or related activity affecting the network performance, the Campus Networking Unit will inform the Computer Lab of the same.

After taking corrective action, the Department or service engineers should inform the Campus Networking Unit about the same so they can turn the port on.

6. Coordination with Campus Networking Unit
Where there is an element of doubt as to whether a particular problem on the computer connected to the Network is related to the Network or the Software installed or Hardware malfunctioning, the Computer Lab/service engineer may coordinate with Campus Networking Unit staff to resolve the problem with joint effort.
This task should not be left to the individual user.

Appendix -C

Ensuring Network Performance

- You must not attempt to intercept, capture, alter, or interfere in any way with information on local, campus, or global network pathways.
- Without authorization, you may not operate Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BootP) servers on the campus networks.
- You must ensure that any device you plan to connect to the Institute network will be compatible with the Network and will operate securely and effectively.
- You must not attempt to obtain system privileges to which you are not entitled, whether on SGGS IE&T Institute resources or systems outside the Institute.
- Computer procedures, programs, websites, and scripts that permit unauthenticated or unauthorized senders to send emails to arbitrary recipients from unrestricted sources are prohibited.
- You must refrain from any action that interferes with the systems' supervisory or accounting functions or is likely to have such effects.
- You must refrain from creating or implementing code intended, even periodically, to interrupt or interfere with networked systems or services.
- You must refrain from knowing the propagation of computer viruses or presumed viruses.
- You must not conduct unauthorized port scans. You must not initiate nuisance or denial-of-service attacks nor respond to these in kind.
- Without authorization from the IT Services department, individuals may not install wireless access points in campus academic, administrative, or service buildings, including hostel buildings. If authorization is provided, the individual must comply with any rules regarding the wireless access point established by the Department.
- Computers, smartphones, and other network devices connected to the Institute's Network are assigned an Internet Protocol (IP) address or, if mobile, "leased" an address by the Institute's network management servers.
- Using other than the assigned IP address can disrupt regular network operation for others, so users and owners of such devices are expected to refrain from supplying some other IP address for use in any network transaction.

Wireless Fidelity (Wi-Fi) Usage Guidelines for students, staff and faculty :

To use Wi-Fi Service, users are supposed to follow the following Instructions.

1. Register user device using user @SGGS IE&T.ac.in mail ID (SGGS IE&T mail ID Only).
   (This is a one-time activity. Users needn't register the same device twice.)
2. If the user doesn't have an email ID, please ask for it in the IT services Section.
3. Do not use registered user device/s using the email of others. This may affect the services of other users.
4. Do not permit others to use a user mail ID to register their device. This may affect user services.
5. Users are allowed to register a maximum of two devices only.
6. To register a user device (s), users should submit details in the Google form available on the Institute website.
7. If a user wants to register a new device, please make sure to de-register the old one.
8. Please check MAC addresses before submitting.

9. Provide these addresses as prescribed in Google Forms only.
10. The user device registration process may take up to one week.
11. If the user's device is not registered in the given period, the user is advised to check user-submitted data.
12. Submit the corrected data using the Google form again.
13. If the user has submitted the corrected data, then there is no problem using services.
14. For any other query or help, the user may contact the admin by writing mail to network admin@sggs.ac.in
15. Ensure users submit the corrected data before contacting IT Services.
16. The above mail ID is the only option to help the user.
17. Remember, Incorrect data is the only reason for connectivity issues.
18. Device registration is for the New users only. Old users needn't register their devices again.
19. Also ensure that the user's mobile handset is configured for a fixed MAC address while connecting to Access Point.

Wireless Fidelity (Wi-Fi) Usage Guidelines for Guests:

To use Wi-Fi Service, Institute Guests are supposed to follow the following Instructions.

1. Submit the user request using the form available on the Website.
2. The user will receive the password; using the password, the user is supposed to connect to the SGGS - Guest SSID.
3. The password is valid for two days.
4. Guest must ensure their device is compliant to connect to the Institute network. They must agree on the IT policy of the Institute.

These guidelines are meant for all members of the SGGS IE&T Network User Community and Guest users of the Institute network.

Due to the increase in hacker activity on campus, Institute IT Policy has put together recommendations to strengthen desktop security.

The following recommendations include:

1. All desktop computers should have the latest version of the antivirus Agent made centrally by the Campus Networking section and should retain the setting that schedules regular updates of virus definitions from the central server.

2. When a desktop computer is installed, all operating system updates and patches should be applied.

In addition, operating system updates and patches should be applied regularly and continuously. The frequency will balance the loss of productivity (while patches are used) and the need for security. We recommend a once-a-week cycle for each machine. Security policies should be set at the server level and applied to the desktop machines whenever possible.

3. All Windows desktops (and OS X or Ubuntu desktops) should have an administrator account that
is not used as the regular login account.

The login for the administrator account should be changed from the default.

4. The password should be difficult to break.

5. Passwords should be changed periodically, and it should be changed when it is suspected that they are known to others.

i. Never use 'NOPASS' as your password
ii. Do not leave the password blank, and Make it a point to change default passwords given by the Software at the time of installation

6. The password for the user login should follow the same parameters outlined above.

7. The guest account should be disabled.

8. New machines with the latest OS (Windows /*Ubuntu/* MacOS, etc.) should activate the built-in firewall.

9. All users should consider the use of a personal firewall that generally comes along the antivirus software if the OS does not have an in-built firewall.

10. All the Software on the compromised computer systems should be re-installed from scratch

11. Do not install Microsoft IIS / any other web server or turn on any of its functions unless necessary.

12. In general, start from a position of security that is most secure (i.e., no shares, no guest access, etc.) and open up services as necessary.

13. Besides the above suggestions, the Campus Networking Unit recommends a regular backup strategy. It should be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise.
Backing up data regularly (daily or weekly) will lessen the damage caused by the loss of a machine.

14. the Campus Networking Unit will shut the port off if a machine is compromised. This will isolate the computer until it is repaired as per the guidelines. At that time, the port will be turned back on.
15. For departments with their subnets and administrators, standard filters can be applied at the subnet level. If a department has its servers, Campus Networking Unit technical personnel can scan the servers for vulnerabilities upon request.

Appendix -D

Managing Electronic Information

- From time to time, members of the Institute community, including students, may use electronic means to collect data of interest to projects or activities that serve a co-curricular purpose unrelated to official Institute business or required academic work.
- Data collected through these means should be considered confidential, and the authors or creators of such surveys or applications must therefore:
  · Provide potential users with a summary of how their data will be collected and maintained.
  · Obtain informed consent concurrent with the user submitting a netid and password.
- Once disclosed, these confidential data also are subject to the requirements described under "Protecting Data" below.
- At no time should the data collected through these means be disclosed in ways that could directly or indirectly identify individuals, and the collectors of this data should take care to protect this confidential information from any unintentional disclosure by adopting all recommended security measures as well as an appropriate plan for data retention and disposal.

Retention and Disposal

- Faculty and staff, including those designated as regular, term, visiting, and temporary, as well as student employees, are responsible for retaining information valuable to the Institute.
- Members of the Institute community, especially employees, should understand that electronic information is governed by the same laws and regulations as paper documents, including statutes protecting the privacy of student records, medical information, and other kinds of personal information.
- Employees and students are expected to apply the same security and record retention practices to electronic information as to paper documents.
- There are three ways of preserving email: on the email system, within an office's paper files, or in some form of electronic record-keeping system,
- Email retained in electronic format must be migrated by the account holder to new Software and storage media as upgrades occur.
- Like all records, many email messages will eventually cease to be helpful or needed by the Department and should be deleted by the account holder.
- When an Institute employee trades in or replaces a computer or other networked device, the employee or the employee's computing support specialist must use appropriate, effective Software to remove any data from the hard drive or, if warranted, destroy the hard drive by means approved by the Institute.
- Email disposal should be regularized and documented as with the disposition of any other Institute records.
- All discarding of media containing SGGS IE&T Institute information must comply with the Information Security Policy.

Official Email

- All members of the Institute community with ready access to email are responsible for knowing the content of official correspondence sent to their Institute-provided email address.
- Students who submit academic work via email should retain copies of the work until sure that the instructor has received a legible copy. Acknowledgment by the instructor of receipt of a legible copy would be courteous and encouraged.

Outside Email

- Faculty, staff, and students with personal email accounts with services outside the Institute should use only their Institute-provided email accounts for communications regarding Institute matters.
- Using Institute email protects the privacy and security of Institute data; allows for verification of sending and receiving critical correspondence regarding academic and other matters; and facilitates responses to subpoenas and other situations that may require the retrieval, inspection, or production of documents, including email.
- Institute account holders who have their email copied or forwarded to an outside account must avoid marking any such copied or forwarded mail as spam for their outside email provider.

Mass Mailings

- At SGGS IE&T Institute, mass electronic mailings are permitted only when authorized by appropriate offices. The same authority would govern email to those constituencies, even if the sender does not use the official list but creates multiple smaller groups to accomplish the same end.
- Without the appropriate Institute authorization, you may not send large mass emails or voice mails.
- Appropriate authorization must also be obtained to conduct web-based or email surveys, whether among members of the campus community or people outside the Institute.
- Surveys related to research and instruction must obtain approval from the Institute's R&D and, in the case of undergraduate study, from the Office of the Dean of the Academics.
- Special approval is not needed for departments seeking feedback on their courses or services nor for recognized organizations canvassing their members.
- "Spamming" is spreading electronic messages or postings widely and without good purpose. "Bombing," sometimes known as "spamming" as well, " is also bombarding an individual, group, or system with numerous repeated messages.
- Both actions interfere with system and network performance and may harass the victims, which, in the case of newsgroups, can number in the thousands.
- Both are violations of Institute regulations. Deliberate replies of this nature will be considered a violation of Institute regulations.

Protecting Data

- Suppose you are responsible for data necessary to the Institute and created or stored on portable devices. In that case, you are also responsible for ensuring the information is backed up regularly in a form that permits ready retrieval.
- If you are a student and have the information needed to complete your Institute academics, you are responsible for maintaining adequate and appropriate data backup.
- Some kinds of information are considered restricted and confidential. Some information is protected by law. Some contractual agreements require the protection of related information. Some research data, including data involving human subjects, must be kept confidential. In general, information should be protected in a way consistent with the Institute's Information Security Policy.
- As an employee or student, whether you have authorized or accidental access to what the Institute defines as restricted or confidential data, you must comply with the Institute's Information Security Policy and know which Institute office has authority over the information.
- You also must confine your access to or viewing of such data to situations in which only your Institute responsibilities require such access or viewing.

- Any handling of confidential data, whether in hard copy, on Institute-owned equipment, or via personally-owned home or mobile devices, should be done in the most secure, confidential manner, consistent with the Information Security Policy.
- In the event of unauthorized access to Institute data, whether through theft or loss of portable devices such as USB drives, laptops, smartphones, or other devices, or any other security breach, the individual who possessed the device or learned of the breach is responsible for notifying the appropriate Institute offices of a potential data breach and assisting with the Institute's data breach response.
- If the individual suspects the breach involves illegal action by a member of the Institute community, the Institute's security policy should be followed.
- Storage services in "the cloud" provide a helpful alternative for those who use portable network devices or have computers stationary in several locations.
- The Institute has arrangements with specific providers for some secure cloud-based services. For example, there are SGGS IE&T ---branded Google Drive accounts subject to the Google Apps for SGGS IE&T Institute Usage Guidelines.

Use of the Institute's Name and Marks

- No individual or organization of the Institute may use SGGS IE&T Institute's name, seal, logos, restricted images, or other identifiers ("marks") or any marks that suggest SGGS IE&T Institute or any other SGGS IE&T Institute organization except to the extent such individual or organization has been authorized by the proper Institute authorities or as permitted under trademark law.
- Deliberate misuse of the Institute's name or other marks by any Institute community member will be considered a serious offense.

Enabling Others

- The privilege of using Institute equipment, wiring, wireless access, computer and Network systems and servers, broadcast media, and access to global communications and information resources is provided to members of the Institute community. It may not be transferred or extended by campus community members to people or groups outside the Institute without authorization.
- This includes providing network service to others through your own Institute network connection. Network service to residential units leased by the Institute may be extended to sublessors only when Institute Housing has approved the sublease.