GSFC University
Academic Division
Office Order No. Provost/052024/84
Date: 30.05.2024

Preamble:

The IT (Information Technology) Policy and Usage Guidelines aim to ensure the effective and responsible use of Information and Communication Technology (ICT) at GSFC University. The Policy and Guidelines can be a valuable tool for improving efficiency, productivity, and communication. However, it also poses risks to the organisation, such as security breaches, data loss and employee misuse. The IT Policy and Usage Guidelines are designed to manage these risks and protect GSFC University's IT assets.

The President, GSFC University approved the IT Policy and Usage Guidelines on May 25, 2024, and the Policy is enclosed as **Annexure - 1**.

All concerned individuals and departments are required to follow and adhere to the IT Policy and Usage Guidelines.

I/C Provost
GSFC University

To:

    All Teaching and Non-Teaching Staff GSFC University

Copy to,

    President Office, GSFC University - For kind information, Please
    Provost's Office, GSFC University
    Director (Adm) & Registrar Office, GSFC University
    Dept. Dir. (Adm) & Director Campus GSFC University
    Dean / Associate Deans - GSFC University
    DOST - AI, Cell
    Finance Division, GSFC University
    Examination Division, GSFC University
    HR Division, GSFC University
    Lab Assistants of Various Computer Labs

GSFC University, Anviksha, P. O. Fertilizernagar, Vadodara - 391750, Gujarat, India
PH.: 0265 - 3093740 E.: info@gsfcuniversity.ac.in W.: www.gsfcuniversity.ac.in

|1

Department of Information Technology Enabled Services
Department of Computer Science & Engineering
Department of Chemical Engineering
Department of F & EHS
Department of Chemical Sciences
Department of Life Sciences
Department of Computer Applications & Data Science
Department of Management Studies & Liberal Arts
Department of Account & Finance
Department of Internship & Placement
Department of Administration
Department of Admission
Select File- Dy. Registrar (I/C), GSFC University

IT Policy
&
Usage Guidelines

- Version 1.0

Doc.No.: GSFCU/IT Policy & Usage Guidelines/Version 1.0

GSFC University

Release Details:

GSFC University IT Policy & Usage Guidelines - Employees / Students –Version - 1.0

| Sr. No	Version Number	Date	Revision Details	Prepared by GSFCU IT	Approved by Dean SOT	Approved by management	Final Approval from Management
1	1.0	25/05/2024	Version 1.0	Mr. J G Simon, SM-IT, GSFCU	Dr Saurabh Shah - Dean, School of Technology	Prof. G R Sinha – PROVOST, GSFCU	Sh. P K Taneja – PRESIDENT, GSFCU

Contents

1. Purpose:

The university owns the equipment, computing and networking resources that are available to support its academic and administrative operations. The university's policies and procedures govern the use of this equipment and technology.

GSFCU's endeavours are to provide all faculty, students and staff with a modern, fully networked computing and IT environment for academic use.

The word "IT resources" in IT policy refers to external storage devices, printers, scanners, desktop computers, AV accessories, portable devices, networks, including wireless networks, Internet connectivity and the software that goes along with them.

These resources are used primarily for GSFC University-related purposes in an ethical way. The purpose of this policy is to set the standard for operation and security, specifically in the context of resource and network access.

IT Infrastructure Model
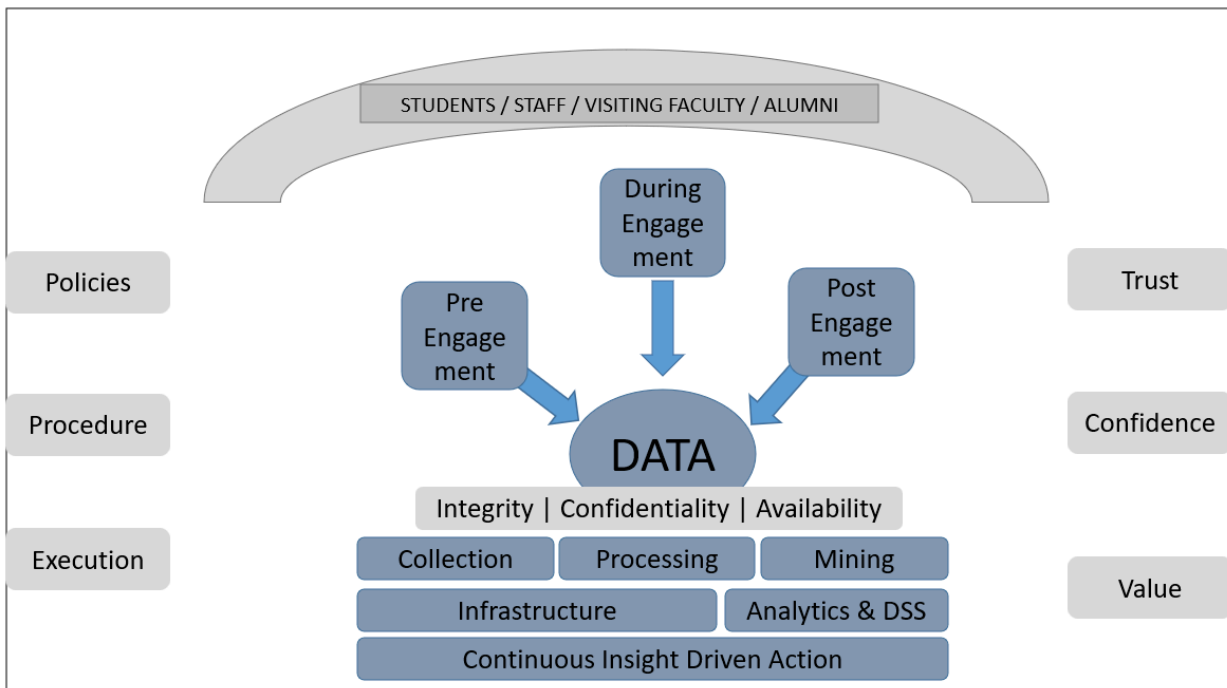
DSS – Decision Support System

2. Scope

- The IT Policy applies to all university faculty, staff and students, as well as all others using the IT resources, whether personally owned or university-owned, that access, transmit or store various types of related information.

- The organisation, including but not limited to computer hardware, software, networks, the internet, email and mobile devices, has IT resources.

- University IT resources must be used to promote the mission of the university in teaching, learning, research and administration.

3. Policy Objective

In particular, the major objectives of this document are:
- To ensure the integrity, reliability, availability and superior performance of the university's IT systems
- To ensure that the IT resources protect the official e-identity (allocated by the university) of an individual
- To ensure that all the users of the university are responsible for adhering to the procedures governing the implementation of this policy document and any other matter incidental to those rules.
- Leveraging information technology as a tool for socio-economic development

A. General IT Ethics:

1. The users of the university shall make effective use of campus systems, the internet, university websites, the Digital Campus System (DCS) and the Learning Management System.

2. The university shall instruct the users that they must comply with university policies and legal obligations (including licenses and contracts).

3. The institution would make an effort to set up awareness campaigns to teach users how to use IT resources efficiently.

4. **Restricted Use:** Users are not permitted to transmit, view or download any content that violates university policy or relevant laws, including but not limited to fraudulent, harassing, obscene, threatening or other messages. It is specifically forbidden to assist in the establishment of a hostile work or academic environment.

5. **Copyrights and Licenses:** Users are required to abide by copyright laws and to honor licenses for content that are protected by copyright. For the sake of clarity, it is against this policy to share information utilizing the university's information resources.

6. **Commercial Use:** The university's IT resources shall not be used for any commercial or promotional purposes, through advertisements, solicitations or any other message-passing medium, except as permitted under university rules.

7. The computing and IT facilities are available for use by faculty, staff and students for official work, academic & research purposes. The usage should not violate any law, institute policy or IT Act 2008 of the Government of India.

8. Users must respect other users' privacy and refrain from giving their password or account access to other parties. It is the user's duty to prevent unauthorized use of their account by changing passwords on a regular basis and using complex passwords. Password sharing is absolutely forbidden for any reason.

9. Users may share the required files through sharing software with a proper access control list.

10. It is against international law to transfer copyright content to or from the GSFCU networks without the owner's prior authorisation. In the event that it is, the user will bear full responsibility.

11. Computer systems may be moved from one location to another with prior written notification to the ITeS Department, as the ITeS Department maintains a record of computer identification. Any deviation from this should be properly documented and given to the ITeS Department.

12. Display of offensive material (either on computer screens or through posters, etc.) is strictly prohibited, and serious action will be taken against offenders.

13. Policy violations shall be handled as appropriately as indiscipline, misdemeanor or academic misconduct. The institute authorities may take action by blocking the account or sending a warning, depending on the seriousness of the infraction. In severe circumstances, the user might not be allowed to use GSFCU's IT resources, their account might be totally erased or it might be reported to the institute's disciplinary action committee, which has been established by the institution's authorities.

B. Acceptable Use
All users of IT resources must follow guidelines for acceptable use. Guidelines include:
1. Internet and email usage: Use IT resources for work-related purposes only.
2. Social media: Use social media for work-related purposes.
3. Remote access: Follow guidelines for remote access, including using secure connections and not sharing login credentials.

C. Hardware Policy
● Users are expected to take proper care of equipment and are expected to report any malfunction to the staff on duty or to the in-charge of the facility. Users should not attempt to move, repair, reconfigure or modify the PC, workstation or smart station.
● Faculty members can use the gadgets inside the classrooms and laboratories only for educational purposes.

D. Software Policy
● Software is Installed using authorized source only.

1. **Open-Source Software:** The University encourages advanced use of open-source software and its effective promotion.
2. **Distribution and Copies:** The University is responsible for making sure that neither the distribution nor the copying of licensed or proprietary software is done illegally.
3. **Software without a license**: You need the ITeS Department's authorisation before downloading and installing any new software without a license. It is totally forbidden to install unauthorized software on GSFCU property or on personal computers linked to the GSFCU network.

E. Network (Internet) Policy

- GSFC University Internet working on the Campus can be accessed for educational and research purposes only.
- Applications supported over the wireless network will be limited as long as this is necessary to provide an acceptable quality of service for all users.
- The use of unauthorized proxy servers and VPN services on the campus network is strictly prohibited. Any attempt to circumvent network security measures through unauthorized proxy servers or VPNs will be considered a serious breach of policy and may lead to disciplinary action.
- Wireless networks will be segmented and treated as "foreign/untrusted networks" from a security standpoint. A firewall or router/switch technology will be employed to provide this segmentation.
- Applications supported over the wireless network will be limited as long as this is necessary to provide an acceptable quality of service for all users.
- Wi-Fi internet availability in hostels and hotspots is available 24 hours a day. The availability of the Wi-Fi signal will vary from place to place.
- Accessing social networking sites such as WhatsApp, Instagram, Facebook, Twitter, etc., is strictly prohibited on campus for personal use. However, subject-handling faculty members can access Google Classroom, MOOCs, Moodle, ERP and other networking sites with permission from ITeS.

F. Email ID Usage Policy

- Employee Email Accounts: All employees are provided with university-issued email accounts for official communication purposes only to the extent possible, users are expected to use only their official email addresses provided by GSFCU.
- It is forbidden to use electronic mail and other network communications facilities to harass, offend or annoy other users of the network, including impeding their computing systems, software or data.
- It is also forbidden to send emails or messages masquerading as another person or to hide the sender's identity. Chain (anonymous origin) letters are not allowed. Neither is any form of commercial advertising or soliciting allowed.
- Do not attach and transmit files (or programs) through email that contain illegal or unauthorized materials.
- Avoid opening Texts and emails from unknown senders as it may contain malicious attachments or links that, when opened, can infect your device with malware or viruses. These malicious programs can compromise your privacy, steal sensitive information or cause harm to your device's functionality.
- Always make it a practice to write a proper subject line and mail body and when attaching a document, the name of the document must be appropriate.
- Spamming is strictly prohibited. Subscribing to mailing lists outside the Institute is an individual's responsibility.

- Subscribing someone else to any group outside GSFCU is illegal.
- Account Creation: Employees must not create email accounts using personal or third-party services for work-related communication without prior authorisation from the IT department.
  - o **Compliance:** All email communications must comply with applicable laws, regulations and university policies.
  - o **Violations:** Violations of this email ID clause may result in disciplinary action, including account suspension or termination, in accordance with university policies."
  - o **Data Confidentiality:** Do not share sensitive or confidential information via email unless encrypted or authorized by appropriate personnel.
  - o **Monitoring:** The Company reserves the right to monitor email communications for security, compliance and legal purposes.
  - o **Reporting:** Employees must promptly report any suspicious or phishing emails to the IT department to mitigate potential security risks.
  - o Do not store Photos and Audio-Video in Google Drive & Photo Storage.
  - o **Storage Quota Allocation:** Each email account will have a specified storage quota assigned based on roles and responsibilities.
    - ➢ Students will get 10 GB during their association with the university.
    - ➢ Students will not be able to access Google Drive & Photos once they have graduated from GSFC University.
    - ➢ Students will be responsible for taking data backup of Google Drive & Photos before service deactivation.
  - o Employee email ID will be deactivated once an employee has left on his/her last day.

G. Data Privacy

All users of IT resources must follow the guidelines for data privacy. The guidelines include:

1. Collecting personal data: Collect personal data only when necessary and with consent.
2. Storing personal data: Store personal data securely and for a limited time.
3. Sharing personal data: Share personal data only when necessary and with consent.
4. Remove any junk files (accidentally installed) immediately to prevent speed bottlenecks.
5. Do not use Internet access to transmit confidential, political, obscene, threatening or harassing materials.
6. Do not download the file(s)/images/videos/songs that are bulky in size, contain material of a pornographic, racist or extreme political nature or incite violence, hatred or any illegal activity.
7. Do not download free, unlicensed software from the Internet and install it on the organization's computer equipment.
8. In case of any data breach of your system, inform ITES immediately after disconnecting the system from the internet.

H. Data Security and Integrity

All users of IT resources must follow security guidelines to protect against unauthorized access, disclosure, modification or destruction of data. The guidelines include:

1. **Passwords:** Use strong passwords and change them regularly.
2. **Access control:** Only access data and systems required for work duties.
3. **Data backup:** Back up data regularly and securely.

4. **Disaster recovery:** Follow procedures for disaster recovery in case of emergencies.
5. The enterprise wireless infrastructure is managed campus-wide by GSFCU IT.

I. Data Audit for ERP
- Regular annual data backup & audit of the ERP is carried out by the ERP
- These data are the basis for all decision-making in the University and, hence, have to be examined for authenticity, relevance, accuracy and completeness with all validations and integration across various modules of DCS.

J. Incident Response
All users of IT resources must follow guidelines for incident response in case of security incidents.
Guidelines include:
1. **Reporting incidents:** Report security incidents immediately to the appropriate IT personnel.
2. **Investigating incidents:** Investigate security incidents to identify the cause and prevent recurrence.
3. **Mitigating incidents:** Take appropriate measures to mitigate the impact of security incidents.

K. IT Service, Hardware & Software Asset Procurement Policy
All users of IT resources must follow guidelines for IT procurement. The guidelines include:
1. Purchasing equipment and software: Purchase equipment and software from reputable vendors.
2. Assessing vendor risks: Assess vendor risks before purchasing equipment and software.
3. Ensuring compliance: Ensure equipment and software comply with established policies and regulations.
4. Create provision for priority up-gradation of the system
5. Create a provision for annual maintenance expenses to ensure maximum uptime for the system.
6. Plan and invest for redundancy at all levels.

L. IT Asset Management
To make it easier for the University to use IT resources on campus, an established business procedure for the management of hardware and software assets is proposed. This will include the protocols for overseeing the acquisition, implementation, upkeep, use and disposal of hardware and software applications inside the institution. The necessary Annual Maintenance Contract (AMC) for each and every asset, wherever required, will be adhered to.

IT Asset Management comprises the following major criteria:

1. Operating System and its Updating: Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through Internet and Active-Directory services. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users

helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by Microsoft for which it provides patches/service packs to fix them. All OS and other software used in the campus must be licensed, no pirated software will be allowed to use in the campus.

2. <u>Antivirus Software and its updating</u>: Computer systems used in the institute should have anti-virus software installed and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy. Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

3. <u>Backups of Data</u>: Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into many volumes, typically C, D and so on. OS and other software should be on the C drive, and the user's data files on the other drives (e.g. D, E). In case of any virus problem, generally, only the C volume gets corrupted. In such an event formatting only one volume will protect the data loss. However, it is not a foolproof solution. Apart from this, users should keep their valuable data on a DVD/Pen Drive or other storage devices such as pen drives or external hard drives.

4. <u>ITeS</u> department, upon finding a non-compliant computer, will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will only be done via DCS complaint or grievance system/email. The individual users will follow up the notification to be certain that his/her computer gains necessary compliance. The ITeS department will provide guidance as needed for the individual to gain compliance.

M. IT Asset Maintenance Policy

Preventive maintenance of the PCs and Peripherals to be carried out once in every three months by Facility Management Service personnel monitored by ITeS Department. The first preventive maintenance would be at the execution stage of the contract and the other after three months.

We carry out preventive maintenance activity once every quarter in addition to the normal maintenance required, and sub-activities are detailed below:

i. Check for any loose contacts in the cable's connections.
ii. Conduct preventive maintenance (including cleaning, inspection, testing, satisfactory execution of diagnostics and necessary repairing of the equipment)
iii. Asset Reconciliation- Efforts will be made to recover the faulty asset, and if it is not possible, then it will be replaced.

- Installation and upgradation of standard software, such as Operating systems, MS-Office, Acrobat Reader, VLC, WinRAR, and other academic-related software, are categorized under Patch Management.

- Computer laboratory Maintenance: All maintenance and upkeep of labs are maintained by the lab in charge including Patch Management. The weekly maintenance report is to be submitted every Monday to the reporting person and concerned division by Lab. In charge.

● Preventive maintenance should be done to the satisfaction of GSFCU. In addition to preventive maintenance, related cleaning of the inside of PCs and printers, cleaning of the outer side of the Keyboards, Mouse, CPU, Monitor and Printer with a proper non-harmful solution should be used in order to remove surface dirt.

N. IT Resource Compliance

All users of IT resources must follow guidelines for compliance with laws and regulations. Guidelines include:

1. **Data protection laws**: Follow data protection laws and regulations.
2. **Intellectual property laws**: Respect the intellectual property rights of others.
3. **Cyber Security**: Installation of a firewall is necessary for superior visibility into risky activity, suspicious traffic and advanced threats helps to regain control of networks. Automatic threat response instantly identifies and isolates compromised systems on the Network to stop threats from spreading.
4. **Disposal of Old Equipment**: To scrap old equipment, the department have to write official letter to the Administration and Administration Manager has to collect the scrap from IteS department and sell it to E-waste management authorized dealer by the Government of Gujarat. The compliance given under GSFCU E-Waste policy must be adhered to.
5. **5-S Implementation**:

    The standard 5S principles (Sort, Set in order, Shine, Standardize, Sustain) must be directly applied to IT resources and data maintained to secure and make them effective.
    A. Identify and remove unnecessary data, software and applications that consume resources and clutter digital spaces and the same applies after the event or program to remove unwanted data / Video / Photos by the program/workshop/meeting coordinator.
    B. Implement clear folder structures and labeling systems for easy file organization and retrieval on your desktop / Laptop.
    C. Clean up your desktop clutter and organize digital files to eliminate distractions and improve workflow.
    D. Regularly assess and address potential security risks to ensure system and data integrity.
    E. Regular system maintenance includes updates, cleaning, and performance optimisation of the IT system.
    F. Take regular backups of your Laptop's/Desktop's data and configurations
    G. Run disk cleanup utilities to remove temporary files and optimize performance

O. Web portal Updating Policy.

● The overall custodian of the web portal would be the IT Head.
● The content/details that are to be uploaded/updated on the portal are to be approved from the head of the respective requesting department and have to be legally compliant as well.
● Further, if any documents are to be uploaded on the web portal or any write up has to be published, the same content/document shall be specifically vetted by the user and the

concerned head. Once the document has been examined, the user shall send the same content/document via email to the ITeS department for further uploading on the portal.

4. Review

University Governance: To fulfill the goals that led to the creation of this policy, the university will make every effort to guarantee that it is applied fairly. The office of the Provost is in charge of overseeing the day-to-day administration of IT resources.

The Provost of GSFC University has approved the IT Policy for GSFC University employees and students.

5. Contact

Comments or questions? Email us at it@gsfcuniversity.ac.in.

The organisation will regularly review and improve IT policies and guidelines to adapt to changing technology, threats and regulations.

The policy may change as and when it is considered appropriate, and new policies or changes in policy will take effect immediately after a brief announcement by any means, including e-mail, printed notices or through the newsgroups.