IT Policy
2024

Gangadhar Meher University, Sambalpur
Amruta Vihar, Sambalpur, Odisha, 768004
gmuniversitysbp@gmail.com

IT Policy

Table of Contents

CONTENTS

1. Statement of Policy: 3
2. ICT Cell Officials 3
3. Applicability: 3
4. Scope of Policy: 3
5. IT Usage and Prohibitions: 4
6. Policy to access Wi-Fi: 5
7. Security and Integrity: 5
8. IT Asset Management: 5
9. IT Hardware Installation Policy: 6

A. Who is Primary User 6

B. What are end user computer systems 6

C. Warranty & Annual Maintenance Contract 7

D. Network Cable Connection 7

E. Non compliance 7

10. Software Installation and Licensing Policy 7

A. Operating System and its Updating 8

B. Backup of Data 8

C. Non compliance 8

11. Misuse: 9
12. Violation of Policy: 10
13. Implementation of Policy: 10

Appendix-I 10

1. STATEMENT OF POLICY:

- To ensure the integrity, reliability, accessibility, and superior performance of the University IT Infrastructure.
- To ensure that the IT resources shields 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 related to those rules.

2. ICT CELL OFFICIALS

Sl. No.	Name with Designation
1	Mr. Ashish Patel, System Manager
2	Mrs. Priyanka Swain, System Manager
3	Mr. Susil Kumar Sahoo

3. APPLICABILITY:

This policy is applicable to all the students & employees of G.M. University, Sambalpur and all others (referred as 'users' in this document hereon) who use institutional Information Technology (IT) infrastructure (i.e. lab components, desktops/laptops, communication nodes, information technology/information, internet facilities and communication technology (IT/ICT) infrastructure etc.), within the University's network and access, transmit or store Institutional and/ or personal information.

4. SCOPE OF POLICY:

IT/ICT resources provided by the University should only be used for the purpose of teaching, learning and research by the users. It is the responsibility of the users to appropriately use and protect institutional IT resources and to respect the rights of others. This policy is a guideline for safer and legitimate use of such IT resources and infrastructure available.

5. IT USAGE AND PROHIBITIONS:

- The users of the University shall make effective usage of internet, wireless resources, official websites (including University website, conference website, journal portals, University Moodle and course website), University Management Systems (UMS) and Swayam/NPTEL portal, Remote Login based facilities of the University and e-Library resources.
- The University shall stress upon the users to comply with institution policies and legal obligations (including licenses and contracts).
- The University shall strive to arrange for awareness programmes to acquaint the users with the effective usage of IT resources.
- Prohibited Use - The users shall not send, view or download fraudulent, harassing, obscene, threatening, or other messages or material that are a violation of applicable law or University policy. In particular, contributing to the creation of a hostile academic or work environment is prohibited.
- Social Media - Users must abide by the rules of the University towards the usage of social networking sites, mailing lists, news rooms, chat rooms and blogs.
- Commercial Use - The University IT resources shall not be used for any commercial and promotional purposes, through advertisements, solicitations or any other message passing medium, except as permitted under institution rules and other uses approved by the competent authority.
- Copyrights and Licenses - Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file-sharing using the University's information resources is a violation of this policy

6. POLICY TO ACCESS WI-FI:

Steps to connect to the campus Wi-Fi network:

Step 1: Search for access ID name: "GM University" on your device and click connect.

Step 2: In the password field enter "GMU@2024".

Step 3: Next user authentication page will open in the browser where you need to enter the user name and password to access the internet (click proceed anyway if any error message appears).

Step 4: Click on the "Login" button to start using internet.

7. SECURITY AND INTEGRITY:

- Personal Use - The University IT resources should not be used for activities violating the basic functionality and mission of the University except in a purely incidental manner.
- The users must refrain from making any unauthorised access of information in order to promote secure access of Network and Computers.
- The competent system administrator may access the information resources for a legitimate purpose.
- Firewall - Additional procedures to maintain a secured flow of internet and intranet-based traffic in the campus shall be managed through the use of Unified Threat management (firewall).
- Anti-virus and security updates - The regular pupation of the anti-virus policy and security updates should be done for the protection of computing resources.

8. IT ASSET MANAGEMENT:

- **Asset Management:** The University shall lay down business processes for the management of hardware and software assets that facilitates the usage of IT resources in the University. This shall include procedures for managing the purchase, deployment,

maintenance, utilization, energy audit, and disposal of software and hardware applications within the University.

- **Copying and Distribution:** The University shall ensure that there is no violation in the copying and distribution of proprietary and licensed softwares.
- **Risks:** The University shall stress on managing the risks involved for the usage of IT resources. This shall include standard procedures for identification, minimization and monitoring of risk impact by protective and corrective measures. This should also include procedures for timely data backup, replication and restoring policies, power backups, audit policies, alternate internet connectivity for a fail-safe internet access. 4.4 Open-Source Asset: The University shall endeavour towards the promotion and effective usage of open source softwares.

9. IT HARDWARE INSTALLATION POLICY

University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

A. WHO IS PRIMARY USER

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be "primary" user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

B. WHAT ARE END USER COMPUTER SYSTEMS

Apart from the client PCs used by the users, the University will consider servers not directly administered by INTERNET UNIT, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the INTERNET UNIT, are still considered under this policy as "end-users" computers.

C. WARRANTY & ANNUAL MAINTENANCE CONTRACT

Computers purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include OS re-installation and checking virus related problems also.

D. 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 the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

E. NON COMPLIANCE

G.M. University faculty, staff, and students not complying with this computer hardware installation policy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computer resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even whole University. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be. Noncompliance of the above may attract a punitive action.

10.SOFTWARE INSTALLATION AND LICENSING POLICY

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.

Respecting the anti-piracy laws of the country, University IT policy does not allow any pirated/unauthorized software installation on the University owned computers and the computers connected to the University campus network. In case of any such instances,

University will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

A. OPERATING SYSTEM AND ITS UPDATING

1. Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers).
2. University as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.
3. Any MS Windows OS based computer that is connected to the network should access http://windowsupdate.microsoft.com web site for free updates.

B. BACKUP OF DATA

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 two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a fool proof solution. Apart from this, users should keep their valuable data either on Floppy, or CD or other storage devices such as pen drives.

C. NON COMPLIANCE

G.M. University faculty, staff, and students not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files inoperable computer resulting in loss of productivity risk of spread of infection to others confidential data being revealed to unauthorized persons

An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even whole University. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

11. MISUSE:

Any usage which contravenes local, state and central government laws or violates norms of GM UNIVERSITY usage will be treated as misuse.

Two specific categories of misuse are listed below. All listed actions and others which effectively amount to the same are considered to be misuse of GM UNIVERSITY's computing, communications and network facility.

Misuse involving or amounting to attack on any devices, systems and/or networks:

- Using the network to gain unauthorised access to any computer system.
- Tapping phone or network transmissions (e.g. running network sniffers without authorisation).
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals or networks.
- Knowingly running, installing and/or giving to another user a program intended to damage or place excessive load on a computer system, network device or network. This includes, but is not limited to, programs known as computer viruses, Trojan horses and worms.
- Attempting to circumvent data protection schemes or uncover security loopholes. 6. Masking the identity of an account or machine.
- Releasing a virus, worm or other program that damages or otherwise harms a device, system or network.
- Using GM UNIVERSITY's resources for unauthorised purposes (e.g. using personal computers connected to the campus network to set up web servers for commercial or illegal purposes).
- Unauthorised access to data or files even if they are not securely protected (e.g. breaking into a system by taking advantage of security holes, or defacing someone else's web page)

12. VIOLATION OF POLICY:

Any contravention of the basic objectives and areas mentioned under the IT Policy of the University shall be considered as a violation and as a misconduct and gross misconduct under University Rules. This may attract a penalty/punitive action, if needed.

13. IMPLEMENTATION OF POLICY:

The University may decide necessary rules to change the policy from time to time which will be effective with prior approval of the competent authority of the University.

APPENDIX-I

Complaint Registration/ Maintenance Form

Name:	Mob:	
Address:	Designation:	
Classroom/Office/Location:	HOD/SO Signature:	
COMPLAINT INFORMATION		
Date and Time of Complaint:		
Nature of Complaint: Networking	Hardware	Software
Product Name & Serial No.		
Brief Description of Complaint:		
Most Convenient Date and Time for availability of user: Signature of Complainant:		

(For Office Use)
Regd. Sr. No/Date: Complaint Taken By: Designation:
Suspected Cause:
What steps should be considered to avoid a repeat of the problem:
Resolved Date & Time:
(Declaration) I hereby confirm that the above complaint has been satisfactorily resolved. Name: Sign: Date:

Director, IQAC
Gangadhar Meher University
Sambalpur

REGISTRAR
GANGADHAR MEHER UNIVERSITY
SAMBALPUR