IT Policy

Sambalpur University,
Jyoti Vihar,
Sambalpur- 768 019

IT Policy

Table of Contents

I. PURPOSE

- The University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.
- This policy establishes University-wide strategies and responsibilities for protecting the **C**onfidentiality, **I**ntegrity, and **A**vailability of the information assets that are accessed, created, managed, and/or controlled by the University.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information

II. OBJECTIVE

- To make information technology accessible to the students and all the teaching and non-teaching staffs of the university.
- To develop and preserve information of all the stake holders of the university.
- To keep information confidential by protecting it from unauthorized personnel.
- The availability of information through round the clock.

III. POLICY COVERAGE

Stake holders on campus or off campus

- Students: UG, PG, Research Scholars
- Employees (Permanent/ Temporary/ Contractual)
- Faculty
- Administrative Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests

IV. IT CELL CORE COMMITTEE MEMBERS

Sl. No.	Designation
1	Vice Chancellor
2	Chairman PG Council
3	Registrar
4	Director, EGOV
5	Director, SUIIT
6	HOD, Computer Science & Applications

7	System In charge, E-Gov Cell
8	Assistant Engineer, Civil
9	JEE, Electrical

V. IT CELL TECHNICAL COMMITTEE MEMBERS

Sl. No.	Name with Designation
1	Prof. P.K.Naik, H.O.D, BT & BI, SU
2	Prof. B.K.Mohanty, Director, SUIIT, SU
3	Dr. C.S.Panda, Director, EGov & H.O.D, CSA, SU
4	Dr. Rajib Padhee, Reader, Dept. of Physics, SU
5	Sri. Arun Basa, Programmer, Computer Centre, SU
6	Sri. Subrat Kar, System Incharge, EGov, SU

VI. RESOURCES

- Network Devices wired/ wireless
- Internet Access
- Official Websites, web applications
- Official Email services
- Data Storage
- Mobile/ Desktop / server computing facility
- Documentation facility (Printers/Scanners)
- Multimedia Contents

VII. IT HARDWARE INSTALLATION POLICY

- **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.

- **Power Connection to Computers and Peripherals**

  All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems

should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

- **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.

- **Maintenance of Computer Systems provided by the University**

  For all the computers that were purchased by the university centrally and distributed by the Estate Branch, University Computer Maintenance Cell (EGOV) will attend the complaints related to any maintenance related problems.

VIII. SOFTWARE INSTALLATION AND LICENSING POLICY

- 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).
- 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.
- Any MS Windows OS based computer that is connected to the network should access http://windowsupdate.microsoft.com web site for free updates. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is users' responsibility to make sure that the updates a being done properly.
- Computer systems used in the university 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 perform regular backups of their vital data.

IX. NETWORK (INTRANET & INTERNET) USE POLICY

- Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the INTERNET UNIT.
- Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or

private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the university.

- Individual departments/individuals connecting to the university 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 INTERNET UNIT in writing and after meeting the requirements of the university IT policy for running such services.
- School, departments, or divisions must register each wireless access point with INTERNET UNIT including Point of Contact information.
- School, departments, or divisions must not operate wireless local area networks with unrestricted access. Network access must be restricted either via authentication or MAC/IP address restrictions. Passwords and data must be encrypted.

X. EMAIL ACCOUNT USE POLICY

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic & other official purposes.

For obtaining the university's email account, user may contact EGOV for email account and default password by submitting an application in a prescribed proforma.

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

- The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
- while sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
- User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
- User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

- While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
- Impersonating email account of others will be taken as a serious offence under the university IT security policy.
- It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.

XI. RESPONSIBILITY OF EGOV

- The campus network backbone and its active components are administered, maintained and controlled by EGOV.
- Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of EGOV.
- Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of EGOV. It essentially means exactly at which location the fibreoptic-based backbone terminates in the buildings will be decided by the EGOV. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fibre optic, wireless or any other media) is also the responsibility of EGOV.
- Every 3 to 5 years, EGOV reviews the existing networking facilities, and need for possible expansion. Network expansion will be carried out by EGOV when the university makes the necessary funds available.
- Where access through Fibre Optic/UTP cables is not feasible, in such EGOV considers providing network connection through wireless connectivity.
- EGOV is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. EGOV monitors the network to ensure that such services are used properly.
- EGOV provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the university upon receiving the requests from the individuals on prescribed proforma.
- EGOV may receive complaints from users/departments, if any of the network related problems are noticed by them during the course of attending the end-user computer systems related complaints. Such complaints should be by email/phone.

- EGOV will be constrained to disconnect any Section, department, or division from the campus network backbone whose traffic violates practices set forth in this policy or any network related policy.

XII. GUIDELINES FOR DESKTOP USERS

- All desktop computers should have the latest version of antivirus such as Symantec Anti-Virus (PC) or Quick Heal and should retain the setting that schedules regular updates of virus definitions from the central server.
- 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, on an ongoing basis. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine.
- All Windows desktops (and OS X or later Macintosh 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.
- The password should be given strong as far as possible so that it will be difficult to break.
- All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall.
- All the software on the compromised computer systems should be re-installed from scratch (i.e. erase the hard drive and start fresh from installation disks).
- 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.
- In addition to the above suggestions, EGOV 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 on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

XIII. VIDEO SURVEILLANCE POLICY

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

- Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.
- Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.
- Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.
- The system has been installed by university with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:
- Detect those having criminal intent.
- Assist in the prevention and detection of crime.
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order.
- Facilitate the identification of any activities/event 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 to provide management information relating to employee compliance with contracts of employment
- The system will not be used to provide recorded images for the world-wide-web.
- The system will not be used to record sound other than in accordance with the policy on covert recording.
- The system will not be used for any automated decision taking.

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:	

Appendix-II

Wi-Fi Registration Form

Sl.No		
1	Name:	
2	Email:	
3	Phone:	
4	Roll No/Registration No/Employee ID:	
5	Hostel:	
6	Student/ Employee:	
7	Department/Section:	
8	Course:	
9	Session:	
10	Desktop MAC:	
11	Laptop MAC:	
12	Mobile MAC:	
13	Antivirus License:	
14	User Name/Login Name:	

Declaration:

1. I will use proper Antivirus for my device.
2. I will not use internet for any activity which are against IT Act and I will be responsible for any misuse.

Date: **Applicant Signature**

Certified the applicant is a student of the Sambalpur University.

(For Office Use Only) **H.O.D**

Form No: **Signature with Date & Seal**