IT POLICY

CENTURION UNIVERSITY OF TECHNOLOGY AND MANAGEMENT, ODISHA

OFFICE: AT/PO: R.SITAPUR, VIA: UPPALADA PARLAKHEMUNDI,
GAJAPATI – 761211, ODISHA (INDIA)

IT Policy

Objectives of IT Policy:

- University IT policy is designed to maintain, secure, and ensure legal and appropriate use of IT infrastructure established by the University on the campus.

- This policy helps University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability (CIA) of the information assets that are accessed, created, managed, and/or controlled by the University.

- Data assets accessed by this policy includes information systems, computers, Firewall, network devices, intellectual property, as well as documents and verbally communicated information

- It is to make all the university operations paperless and thereby reduce carbon footprint and achieve green computing.

- Towards this goal, we are in the process of developing and deploying learning management system (LMS) and enterprise resource planning (ERP) solutions. It includes making educational teaching material available online for teachers, as well as tutorials for students.

Over the last decade, active users accessing the network facilities have increased rapidly along with web-based applications. This is a welcome change in the university's academic environment. Now, the university has about 4000 network connections covering all buildings across the campuses and expected to reach 9000 plus connections.

MIS Cell is the department that has been given the responsibility of running the university's intranet & Internet services.

Internet Unit is running the Firewall security, Proxy, DHCP, DNS, email, web and application servers and managing the network of the university.

CUTM is getting its Internet bandwidth from JIO with 1 Gbps connectivity shared across the campuses.

A central committee gathers requirements from various departments and prepares an integrated IT plan. Senior management approves the same, along with its budgetary requirements, and provides necessary funds in a timely manner as per an approved schedule. To keep the costs low, as well as to ensure faculty enhance their skills and students learn the latest technologies,

CUTM does most of its custom application development in house. For example, LMS solution is being developed in-house by customizing and enhancing open source Sakai LMS and BigBlueButton web conference technologies.

IT Policy

IT policies may be classified into following groups:

- Computer Network Hardware Policy
- Installation of the software with Licensing Policy
- Use of network (Intranet & Internet) Policy
- E-mail Account Use Policy

IT policy is applicable to

- All Students: UG, PG, Research (Hostellers and Day Scholars
- Employees / Faculty / Administrative Staff (Permanent/ Temporary/ Contractual), Higher Authorities and Officers including Guests

□□□Computer Network Hardware Policy

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

A. Warranty & Annual Maintenance Contract

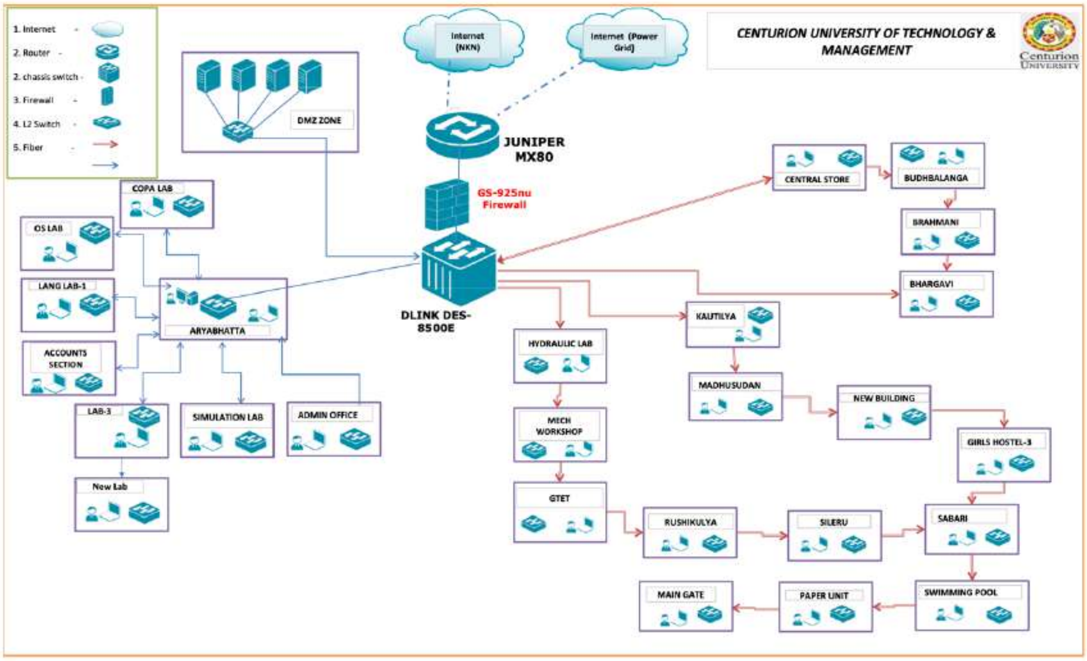
Computers purchased by any Section/Department/Project should preferably be with 3-year on- site comprehensive warranty. After the expiry of warranty, computers will be under annual maintenance contract. Maintenance includes OS re-installation and checking virus related problems also.

B. Power Connection to Computers and Peripherals

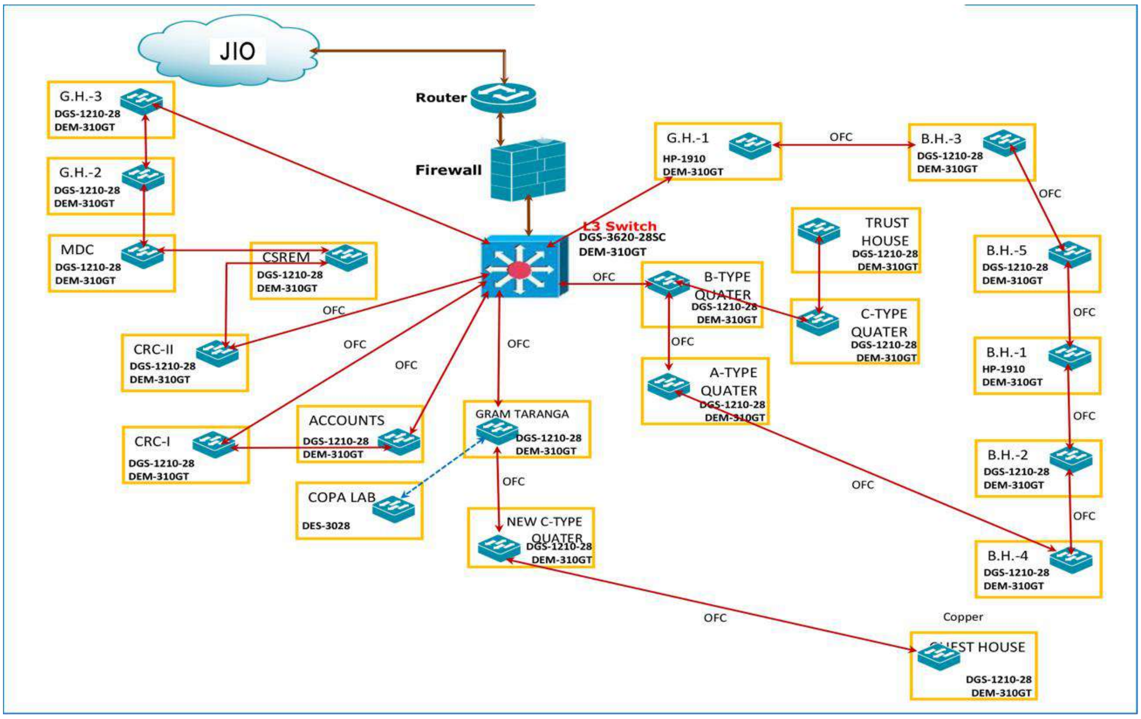
All the computers and peripherals are connoted to the electrical point strictly through online UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging and discharging during the power cut. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

C. Network Connectivity

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. NO other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected. Campus Network Connectivity is shown below



BBSR Campus



JITM

D. Moving Computer from One Location to another and Maintenance
Computer system may be moved from one location to another with prior written intimation to the MIS cell from the concern HODs or Deans, as they will be maintaining all information of computer names and its IP address. Such computer names follow the convention that it comprises year of purchase, department, floor and room number

E. High performance computing (HPC):
PARAM Shavak Supercomputers have been procured for performing high-end scientific research using modelling, simulation and data analysis, and creating HPC aware skilled workforce. We have two of such type one is in Jatni campus and the other is in Parlakhemundi campus. Geotagging images is given below

Processor - Intel xenon Gold 6132(Skylake), 14 corers with 2.6GHz Clock
Ram - DDR4 - 96GB
Graphics - Nvidia Quadro P5000(PARAM Shavak VR) 15GB GDDR5X, Nvidia Quadro P400 2GB GDDR5
Storage- 16TB RAID5 Configured
1KWatt Power Supply.

Rajaseetapuram, Odisha, India
CUTM Library, Server Room, Odisha 761211, India
Lat N 18° 48' 23.8392" Long E 84° 8' 23.1936"
09/02/21 03:28 PM
0.0° C
179° S
33.0 μT
Google

These two computers are used for rendering of 3d videos for students for easy understanding of the subjects. It is also used for processing of Hyper Spectral images from Hyper Spectral cameras and will be used further for algorithms in AI / ML.

II. Installation of the software with Licensing Policy

Any computer purchased by an individual departments/projects should make sure that computer systems must have all licensed software including Operating System, Antivirus and necessary software’s installed.
Respecting the anti-piracy laws of the country, University IT policy will not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network. If found university will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals’ rooms.

Operating System and its Updating

Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them.

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 Microsoft OS based computer that is connected to the network should access https://microsoft.com web site for free updates. Such updating should be done with automatic updates, it is users responsibility to make sure that the updates a being done properly.

Antivirus Software and its updating

Computer systems used in the university having Microsoft OS are mandate to have anti-virus software installed, and it should be active at all times. Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

III. Use of network (Intranet & Internet) Policy

IP Addressing to end users

Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the network administrator / Engineer. Each Department has a pool of ip addresses and each computer in the department will be given an Ip address belonging to that group. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorizedly from any other location. IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

DHCP and Proxy Configuration by Individual Departments /Sections/ Users

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch and distributing IP addresses (private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the university. Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration.

Wireless Local Area Networks

This policy applicable to all the departments and other administrative blocks which are inside the campuses. In addition to the requirements of this policy, each department must register each wireless access point with MIS cell.

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.

IV. E-mail Account Use Policy

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. E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to `http://gmail.com` with their email `ID` and `password`. For getting the university's email account, user may contact MIS Cell for email account and default password after getting their registration number. By default registrationnumber@cutm.ac.in is the email id given to all students till they get the original Degree Certificate.

Those who are using the email should remember the following points:

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 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.
3. User should keep the mail box used space within about 95% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
4. User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it.
5. 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.
6. . Impersonating email account of others will be taken as a serious offence under the university IT security policy.
7. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.

The IT policy also includes management of several of its current infrastructure:
1) Firewall: A Service Gateway Management Group (MID) is used to add and remove firewall administrators, and manage their "Security" rights. Students, faculty, and staff

can contact any of its members in case of any problems in accessing any web resources, etc.

2) Core network - Both wired and wireless: Both remote and on-site troubleshooting is provided for GSM/CDMA and NGN products.

3) Secure campus-to-campus connectivity: VPN is used for such connectivity over a public network such as the Internet.

4) Server Administration: It involves installation, configuration, and maintenance of servers, routers, switches, PCs, etc., apart from user account management, monitoring their performance, and carrying out backup and recovery operations. For example, for backup and disaster recovery policy, it involves deciding what is backed up, how often, how is it stored and secured, how is it restored, etc.

6) Cloud services: For online storage of data, including large digital media, cloud services such as AWS are used extensively. A cloud policy module describes what to migrate to cloud, how to ensure it is secure.