MANAGEMENT EDUCATION AND RESEARCH INSTITUTE

The Policy and the Procedure for maintaining and utilizing Physical academic and the support facilities

The physical facilities including Lab, Classrooms and auditorium etc. are made available for the students those who are admitted in the college. The classrooms boards and furniture facilities are utilized regularly by the students but sometime it is also made available for the other governmental and the non-governmental organizations for conducting the exams etc. if not in use for the said period. The academic support facilities like library, the sports and the other platforms supporting overall development of the students. is open to the college students and other stakeholders.

- The maintenance and the cleaning of the classrooms , laboratories, auditorium etc are to be done through contractual staff through maintenance contract to local experts and supervised by supervisor
- Sports facilities are to be made available to students through the sports coordinator who is also responsible for maintaining them together the maintenance supervisor
- The college garden is to be maintained by the gardener appointed by the institute.
- Electrical and the Plumbing related maintenance is done with the help local skilled persons and the expenditure is done from budget.

IT Infrastructure

IT infrastructure utilization and maintenance is to be as per IT Policy

Need for IT Policy

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

Undoubtedly, Intranet & Internet services have become most important resources in educational institutions & research organizations. Realizing the importance of these services, institute took initiative way back in 2004 and established basic network infrastructure in the institute .

Over the last ten years, not only active users of the network facilities have increased many folds but also the web-based applications have increased. This is a welcome change in the institute’s academic environment.

IT department that has been given the responsibility of running the Institute’s intranet & Internet services

The department is running the Firewall security, Proxy, DHCP, DNS, email, web and application servers and managing the network of the institute.

Institute is getting its Internet bandwidth from BSNL, Reliance, Airtel Total bandwidth availability is 32 Mbps .

Applies to

Stake holders on campus or off campus

- Students
- Faculty
- Administrative Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests

IT Hardware Installation Policy

Institute 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. **Warranty & Annual Maintenance Contract**

Computers purchased by the Department 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.

C. **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.

D. **File and Print Sharing Facilities**

File and print sharing facilities on the computer over the network should be installed.

E. **Maintenance of Computer Systems provided by the University**

For all the computers the compute centre incharge will attend the complaints related to any maintenance related problems.

F. COMPUTER CENTER Interface

IT department upon finding a non-compliant computer affecting the network, will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone . The department will provide guidance as needed for the individual to gain compliance.

Software Installation and Licensing Policy

Any computer purchases made by the departments 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, IT policy does not allow any pirated/unauthorized software installation on the institute's owned computers and the computers connected to the campus network. In case of any such instances, institute 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). 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. Checking for updates and updating of the OS should be performed at least once in a week or so.

2.Institute 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. 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.

B. Antivirus Software and its updating

1. 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.

2. Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from any service-providing agency.

C. Backups 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 foolproof solution. Apart from this, users should keep their valuable data either on pendrives, or CD or other storage devices

Network (Intranet & Internet) Use Policy

Network connectivity provided through the institute, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the IT Policy. The IT department 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 the department.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the network, should have an IP address assigned by the department.

An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports. IP address for each computer should be obtained separately.

B. 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/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 institute.

Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by the IT department. Even configuration of any computer with additional network interface card and connecting another computer to it is considered as 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. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

C. 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 department in writing and after meeting the requirements of the IT policy for running such services. Non-compliance with this policy is a direct violation of the IT policy, and will result in termination of their connection to the Network.

IT department takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property.
IT department 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 a institute’s network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the institute Network connects. The network and computer resources are not to be used for personal commercial purposes.
Network traffic will be monitored for security and for performance reasons .
Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection

D. Wireless Local Area Networks

1. This policy applies, in its entirety to department wireless local area networks. In addition to the requirements of this policy, departments must register each wireless access point with IT department .

2. Departments must inform IT department for the use of radio spectrum , prior to implementation of wireless local area networks.

3. Departments 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.

Email Account Use Policy

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

Web Site Hosting Policy

1. Official Pages

Departments, and Associations of Teachers/Employees/Students may have pages on Institute’s Intranet Channel of the official Web page.

Official Web pages must conform to the institute Web Site Creation Guidelines for Web site hosting.

As on date, the institute’s webmaster is responsible for maintaining the official web site

Affiliated Pages:

Faculty may host Web pages for "affiliated" professional organizations on department Web servers as long as adequate support and resources are available. Prior approval from the competent administrative authority must be obtained for hosting such pages. Individual units reserve the right to discontinue the service and will provide reasonable advance notice to that affiliated organization.

2. Web Pages for eLearning

Though the university does not have this facility as on this date, this Policy relates to future requirements for Web pages for eLearning authored as a result of Teaching/Learning process.

Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the Web, linked through the appropriate department's pages.

Because majority of student pages will be published on the Institute's Web for eLearning, it must reflect the academic mission, and be careful that the published material is not misrepresentative in any way by conflicting with official institute or other Web sites. The following are the storage and content requirements for class-generated student Web pages:

Servers:

It is recommended that pages be placed on the student information server, but pages developed for classes also may be placed on departmental servers or the main campus server meant for eLearning purpose.

Maintenance:

If the pages are published on the eLearning information server, they will be maintained under the default rules for personal eLearning pagesThe instructor will maintain pages that are published on departmental servers or the main campus server meant for eLearning purpose.

Content Disclaimer:

The home page of every class-generated site will include the instute's Content Disclaimer (for pages published on the eLearning information server, the content disclaimer should be generated automatically):

Class Information:

The home page of every class-generated site will contain the name of the class, the student's name, the date, and a link to the class home page.

Official Pages:

If Web pages developed for eLearning become the part of the "official" institute's page, they must be removed from the eLearning information server, departmental servers as class-generated pages (students, can of course, link to their work from their personal student pages).

Responsibilities of University Computer Center

A. Maintenance of Computer Hardware & Peripherals

COMPUTER CENTER is responsible for maintenance of the computer systems and peripherals that are either under warranty or annual maintenance contract.

B. Receiving Complaints

COMPUTER CENTER may receive complaints , if any of the particular computer systems are causing network related problems.

COMPUTER CENTER may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems.

The designated person in COMPUTER CENTER receives complaints from the users 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.

C. Scope of Service

COMPUTER CENTER will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the university and was loaded by the company.

D. Installation of Un-authorised Software

COMPUTER CENTER or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

E. Reporting IT Policy Violation Incidents

If COMPUTER CENTER or its service engineers come across any applications that are interfering with the network operations or with the IT policies o, such incidents should be brought to the notice of the IT department and university authorities.

F.Budgeting and Procurement of Softwares and hardware

The Centre will prepare budget for updation of software/ hardware and present it to the department for further approval. The centre will coordinate with faculty for software requirement and purchase latest softwares.

Responsibilities of Departments

A. User Account

Any department or other entity can connect to the Institute’s network using a legitimate user account .Once a user account is allocated for accessing the network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the institute for all the actions performed using that user account. Hence, users are advised to take reasonable measures such as using complex passwords, not sharing the passwords with others, not writing down the password at a place which is accessible to others, changing the passwords frequently and keeping separate passwords for Net Access Id and for email account ID) to prevent un-authorised use of their user account by others.

It is the duty of the user to know the IT policy of the university and follow the guidelines to make proper use of the university's technology and information resources

C. Supply of Information by Departments, or other entity for Publishing /updating the Web Site

All Departments should provide updated information concerning them periodically (at least once in a month or earlier).

D. Setting up of Wireless Local Area Networks/Broadband Connectivity

1. This policy applies, in its entirety, to departments wireless local area networks/broadband connectivity within the academic complex. In addition to the requirements of this policy, departmentsmust register each wireless access point with IT department

2. Obtaining Broadband connections and using the computers alternatively on the broadband and the institute's campus-wide network is direct violation of the institute's IT Policy. IT Policy does not allow broadband connections within the academic complex.

3. Departments 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.

E. Security

In connecting to the network backbone, a department agrees to abide by this Network Usage Policy under the IT Security Policy. Any network security incidents are resolved by coordination with a Point of Contact in the originating department. If a POC is not available to contact, the security incident is resolved by disconnecting the offending computer from the network till the compliance is met by the user/POC.

F. Preservation of Network Equipment and Accessories

Routers, Switches, Fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries that are installed at different locations by the university are the property of the university and are maintained by Computer centre.

J. Enforcement

Computer centre periodically scans the network for provisos set forth in the Network Use Policy. Failure to comply may result in discontinuance of service to the individual who is responsible for violation of IT policy and guidelines.

Guidelines for running Application or Information Servers

Running Application or Information Servers

i Departments may run an application or information server.

ii Individual faculty, staff or students on the campus may not run personal, publicly available application or information servers (including content or services providing programs such as ftp, chat, news, games, mail, ISP, etc.) on the network.

Responsibilities for Those Running Application or Information Servers

Departments may run an application or information server. They are responsible for maintaining their own servers.

1) Application or information server content and services must follow content guidelines as described in the Guidelines

2) Obtain an IP address to be used on the server

3) Get the hostname of the server entered in the DNS server for IP Address resolution.

4) Make sure that only the services that are essential for running the server for the purpose it is intended for should be enabled on the server.

5) Make sure that the server is protected adequately against virus attacks and intrusions, by installing the appropriate software such as anti-virus, intrusion prevention, personal firewall, anti-spam etc.

6) Operating System and the other security software should be periodically updated.

7) Departments may run an application or information server provided they do the following:

I. Provide their own computer, software and support staff

II. Provide prior information to computer centre on installing such Servers and obtain necessary IP address for this purpose.

Video Surveillance Policy

1.0The system

1.1 *The system comprises: Fixed position cameras.*

1.2 Cameras will be located at strategic points on the campus. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

1.3 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.

2.0 Purpose of the system

2.1 The system has been installed by institute with the primary purpose of reducing the threat of crime generally, protecting 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:

- Deter 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

3.0 Recording

3.1 Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

3.2 Images will normally be retained for fifteen days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

3.3 All hard drives and recorders shall remain the property of institute until disposal and destruction.

4.0 Access to images

4.1 All access to images will be recorded in the Access Log

4.2 Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.

4.3.0 Access to images by third parties

4.3.1 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 enquiry and/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 enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident

4.4.0 Access to images by a subject

CCTV/IP Cemera digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by C.C.T.V. /IP Cemera is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right of instant access.

4.4.1 A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the IT Department

.

4.4.1 The department has the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

5.**0 Request to prevent processing**

5.1 An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

5.2 All such requests should be addressed in the first instance to the IT department, who will provide a written response within 21 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

6.0 Complaints

6.1 It is recognised that members of institute and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in to the IT department .

Library- Utilisation and Maintenance

1. The Library will remain open on all working days from 8.30 AM to 7.00 PM unless otherwise specified by the management.
2. The Library will remain closed from 2.00 PM to 2.30 PM for Lunch.
3. Books will be issued and returned on all working days during the library timings mentioned above.
4. Magazines, Periodicals, News paper, Reference material, Project reports and rare books will be issued only for reading within the Library.
5. It will be incumbent on the member to produce Identity card at the counter when so demanded.
6. Every member will write his/her name, class, section, roll number in the register at the entrance and put his/her signature whenever entering the library.

7. All personal items including books are prohibited from being taken inside the library which may be left at the property rack at the sole risk and responsibility of the student themselves.
8. SILENCE will be strictly observed in the library or else students found guilty will be asked to leave the Library.
9. Each student will be issued 4 Library cards, one book against each card can be issued at a time. These card will have to be surrendered while leaving the Institute.
10. Books will be issued for one week and can be reissued for another one week unless required by another student. After two weeks, the book will be returned and can be reissued only after a gap of two days.
11. All issued books should be returned as on due date by the students. If the due date happens to be a holiday, the book will have to be returned on the next working day, failing which fine will be charged.
12. A fine of Rs. 10/- per day per book will be charged for the delay in returning the book after the due date.
13. The Librarian can suspend issue of books at any time if required.
14. The Librarian can recall issued books at any time if needed.
15. Library cards are not transferable and misuse will attract fine and/or disciplinary action.
16. Members must check and fully satisfy themselves about the physical condition of the book before taking the book out of the library and also check existence of all the pages in the book. Number of pages and physical condition will be checked while returning the book. If the pages are found missing/damaged the member will be fined or asked to replace the book. Members are advised not to write any thing in the book.
17. A member loosing the card will make a written request to the librarian and a duplicate card will be issued on payment of Rs.30/-for each lost card.

18. If nay student is found in book hiding, stealing or mutilating he/ she will be fined as under:

Book hiding : Rs. 100/- plus suspension from the library for a week

Damaging the book : To pay double the cost of the book

Stealing : Rs. 500/- plus one month suspension from the use of
Library.

Misbehavior with staff : Suspension for one month from the use of library
besides other disciplinary action .

19. In case a library member has lost an issued book he/she will be required to pay double the cost of the book.
20. Stock verification of the books will be undertaken at least once every year in the month of May/June. The short fall, if any found will be accounted for by the library staff.

The library is to be maintained by library staff and activities like fumigation and keeping library clean is to be done frequently by library staff.