IT Policy

Prepared by:

Dr. Hiren Dand

Ms. Shilpi Jawake

Ms. Shreya Shenoy

November 2020

Table of Contents

1. Importance

In this digital eon, Information Technology (IT) services stand to be among the most crucial utilities for any educational institution and research organization. Avoiding inappropriate or illegal internet usage or software is the need of the hour. Such technical incongruities creates risks for our organization's lawfulness and repute. IT withholds the responsibility to handle and safeguard the organization against these cyber misconducts.

Last 2 decades have seen an exponential growth in number of the active users for the networking utilities as well as various web-based applications. IT ensures an effective management of these by implementing various functionalities such as Firewall security, Proxy, DHCP, DNS, email, web application servers etc. Effective internet management is critical as too many concurrent users create stress on the Internet Bandwidth available. Non-essential downloads may clog the traffic, resulting in poor Quality of Service (QoS) thus affecting the genuine clients and users of the applications. PTVA's Mulund College of Commerce (MCC) focuses efficient utilization of the Internet bandwidth so as to ensure the full-time access and availability to the unpretentious clients.

Security from viruses, worms, Trojans and various other cyber-attacks needs to be addressed proficiently as they may compromise critical systems and data stored in files or on server. Effects of such cyber miscreants may range from as simple as a damage or corruption of a file to as severe as bringing down the entire network to a standstill. Users fall prey to such Malwares through easy infectious links sent via email which may cause a forced encryption or an entire lockdown of the IT equipment. If not prevented well in advance, a considerable amount of crucial time needs to be spent on the restoring activity of the workstation being attacked.

IT needs to secure the systems and network by incorporating and implementing various steps such as installing firewalls and monitoring logs through automated tools, having access control mechanisms and use of AI to optimise prevention of virus intrusion and content filtering software at the perimeter gateway.

All this is ensured precisely with the help of a clearly defined IT policy in place otherwise it is extremely difficult to convince users about the steps that are taken for managing the network and systems. Many a times users tend to feel that such restrictions are unwarranted, unjustified and infringing the freedom of use. Almost

all the organizations today have an effective IT policy implemented in their respective institutions. This is true for the educational institutions worldwide. In absence of strong management policies, IT security measures will not be effective and not necessarily align with institution's objectives and goals. Hence, policies and guidelines form the foundation of the Institution's security management programme.

Effective policies warrant and exhibit institution's conscientiousness; often necessary in the event of an IT audit or litigation. Hence, it is important to have a well-defined and adept formal IT policy in order to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by MCC on the campus. Our IT usage policies outline our procedures for using internet connection, Network and all the IT equipment's in the college campus.

This policy establishes strategies and responsibilities for protecting the Confidentiality, Integrity, Access Control and Availability, which are the core principles of security, of the information assets that are accessed, created, managed, and/or controlled by MCC. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information (via VOIP) within the campus network.

Policies also serve as outlines that help the institution to implement security measures effectually and proficiently. An agile security policy is as necessary to a good information security program as a solid foundation to the building.

Hence, MCC also is proposing to have its own IT Policy that works as guidelines for using the MCC's computing facilities including computer hardware, software, email, information resources, Network - intranet and Internet access facilities, collectively called "IT POLICY".

2. Purpose and objectives

Availability and quality of information in an enterprise are determined by the type of IT infrastructure and implementation strategy for IT policy. Only a cost-effective IT infrastructure that focuses on a set of well-defined objectives of the IT policy can serve the broad objective of managerial effectiveness.

Important objectives of IT policy for a modern enterprise have been defined below:

1. To provide IT infrastructure that would enable the users identify opportunities, improve performance, and understand business environment.
2. To develop and preserve information as corporate resource and to offer infrastructure to ensure coherent access for users to complete, concise and timely information.

3. Scope of the policy

People to Whom Policy Applies: This Policy applies to everyone who accesses Institute Information Technology Resources, whether affiliated with the Institute or not, whether on campus or from remote locations, including but not limited to students, faculty, staff, contractors, consultants, temporary employees, guests, and volunteers. By accessing Institute Information Technology Resources, the user agrees to comply with this Policy.

Definition of Information Technology Resources: Information Technology Resources for purposes of this Policy include, but are not limited to, Institute-owned transmission lines, networks, wireless networks, servers, exchanges, internet connections, terminals, applications, and personal computers. Information Technology Resources include those owned by the Institute and those used by the Institute under license or contract, including but not limited to information recorded on all types of electronic media, computer hardware and software, paper, computer networks, and telephone systems. Information Technology Resources also includes, but is not limited to, personal computers, servers, wireless networks and other devices not owned by the Institute but intentionally connected to the Institute-owned Information Technology Resources (other than temporary legitimate access via the world wide web access) while so connected.

4. Approval and effective date

This policy has been approved by standing committee of the college in its meeting on _____ and shall be effective from _____.

5. Rules, guidelines and regulations relevant to this policy

This policy document has been prepared keeping in view various rules, guidelines and regulations that have a bearing on contents of this policy. Following are highlights of these including the consequences such as penal action.

5.1 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. What are End User Computer Systems?

Apart from the client PCs used by the users, the Institute 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. 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.

E. 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.

F. File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

G. Shifting Computer from One Location to another

Computer system may be moved from one location to another with prior written intimation to the INTERNET UNIT, as INTERNET UNIT maintains a record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building name abbreviation and room No. As and when any deviation (from the list maintained by INTERNET UNIT) is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified . When the end user meets the compliance and informs INTERNET UNIT in writing/by email, connection will be restored.

H. Maintenance of Computer Systems provided by the Institute

For all the computers that were purchased by the Institute centrally and distributed, Institute Computer Maintenance Cell (COMPUTER CENTER) will attend the complaints related to any maintenance related problems.

I. Noncompliance

MCC 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 Institute. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

J. INTERNET UNIT/COMPUTER CENTER Interface

INTERNET UNIT 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 and a copy of the notification will be sent to the COMPUTER CENTER, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The INTERNET UNIT will provide guidance as needed for the individual to gain compliance.

5.2 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, Institute IT policy does not allow any pirated/unauthorized software installation on the Institute owned computers and the computers connected to the Institute 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. All 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.
3. 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 Floppy, or CD or other storage devices such as pen drives.

D. Noncompliance

MCC 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 affects on other individuals, groups, departments, or even whole Institute. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

E. INTERNET UNIT/COMPUTER CENTER Interface

INTERNET UNIT 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 be done via email/telephone and a copy of the notification will be sent to the COMPUTER CENTER, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The INTERNET UNIT will provide guidance as needed for the individual to gain compliance.

5.3 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 Institute IT Policy. The Communication & Information Services (INTERNET UNIT) 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 INTERNET UNIT.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the Institute network, should have an IP address assigned by the INTERNET UNIT. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided. So, any computer connected to the network from that building will be allocated IP address only from that Address pool. 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.

As and when a new computer is installed in any location, the concerned user can download the application form available for the purpose of IP address allocation and fill it up and get the IP address from the INTERNET UNIT.

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 by filling up a requisition form meant for this purpose.

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 INTERNET UNIT.

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

INTERNET UNIT takes no responsibility for the content of machines connected to the Network, regardless of those machines being Institute or personal property.

INTERNET UNIT 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. Institute network and computer resources are not to be used for personal commercial purposes.

Network traffic will be monitored for security and for performance reasons at INTERNET UNIT.

Impersonation of an authorized user while connecting to the Network is in direct violation of this policy and will result in the termination of the connection.

D. Dial-up/Broadband Connections

Computer systems that are part of the Institute’s campus-wide network, whether Institute’s property or personal property, should not be used for dial-up/broadband connections, as it violates the Institute’s security by way of bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

E. Wireless Local Area Networks

1. This policy applies, in its entirety, to School, department, or division wireless local area networks. In addition to the requirements of this policy, school, departments, or divisions must register each wireless access point with INTERNET UNIT including Point of Contact information.
2. School, departments, or divisions must inform INTERNET UNIT for the use of radio spectrum , prior to implementation of wireless local area networks.
3. 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.
4. If individual School wants to have inter-building wireless network, prior to installation of such network, it should obtain permission from the Institute

authorities whose application may be routed through the Co-ordinator, INTERNET UNIT.

F. Internet Bandwidth obtained by Other Departments

Internet bandwidth acquired by any Section, department of the Institute under any research programme/project should ideally be pooled with the Institute's Internet bandwidth, and be treated as Institute's common resource.

Under particular circumstances, which prevent any such pooling with the Institute Internet bandwidth, such network should be totally separated from the Institute's campus network. All the computer systems using that network should have separate

IP address scheme (private as well as public) and the Institute gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the Institute IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to INTERNET UNIT.

Non-compliance to this policy will be direct violation of the Institute's IT security policy.

5.4 Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the Institute's administrators, it is recommended to utilize the Institute's e-mail services, for formal Institute communication and for academic and 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 Institute communications are official notices from the Institute to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general Institute 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 https://outlook.live.com/ with their User ID and password. For obtaining the

Institute's email account, user may contact INTERNET UNIT 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:

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 Institute'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. while sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4. User should keep the mail box used space within about 80% 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.
5. 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. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.
6. Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.

7. 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.
8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
9. 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.
10. Impersonating email account of others will be taken as a serious offence under the Institute IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of Institute's email usage policy.
12. Any Spam mail received by the user into INBOX should be forwarded to spam@mccmulund.ac.in
13. Any mail wrongly stamped as SPAM mail should be forwarded to wrongspam@mccmulund.ac.in
14. All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. If so, user may forward that mail ID to netadmin@mccmulund.ac.in for necessary action to delete from the spam mail category. It is recommended to empty this folder as frequently as possible.

The above laid down policies particularly 1 to 11 are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.com etc., as long as they are being used from the Institute's campus network, or by using the resources provided by the Institute to the individual for official use even from outside.

5.5 Web Site Hosting Policy

Official Pages

Sections, departments, and Associations of Teachers/Employees/Students may have pages on MCC'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 of the Institute viz., https://www.mccmulund.ac.in only.

Personal Pages:

The Institute computer and network infrastructure is a limited resource owned by the Institute. It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal pages linked to official web site of the Institute by sending a written request to INTERNET UNIT giving the details of the hyperlink of the URL that he/she wants to be added in the official web site of the Institute. However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws. Personal pages also will not include the hosting of pages for other individuals or groups.

Personal pages should explicitly mention that views expressed by him/her in their pages are exclusively their own and not that of the Institute.

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.

Web Pages for eLearning

Though the Institute 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 MCC or other Web sites. If a student publishes a fictional Web site or a Web site modeled after an existing institution or corporation, the site must be clearly identified as a class project.

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 pages

The 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 MCC 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.

Pages Generated by Class Groups:

Pages produced by class groups, if placed on the eLearning information server, will be placed on the server under the name of the designated group leader.

Official Pages:

If Web pages developed for eLearning become the part of the "official" MCC 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).

Student Web Pages

Though the Institute does not have this facility as on this date, this policy relates to future requirements for personal student Web pages. Policies for student pages authored as a result of academic assignments are in II above. It is recognized that each individual student will have individual requirements for his/her pages. As the Institute's computer and network infrastructure is a limited resource owned by the Institute, only web pages of students related to their assignments will be accepted on the Students web pages. The contents of personal pages hosted by the students even on outside web site must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws.

The following are the storage and content requirements for personal student Web pages:

Servers:

Pages will be placed on the student information server.

Maintenance:

Pages published on the student information server will be maintained under the default rules for personal student pages.

Content Disclaimer:

Every personal page will include the MCC Content Disclaimer (the content disclaimer will be generated automatically):

Responsibilities for Those Maintaining Web Pages

Sections, departments, units, and individuals are responsible for maintaining their own Web pages.

MCC Web pages (including personal pages) must adhere to the MCC Web Page

Standards and Design Guidelines and should be approved MCC WebPages Advisory Committee.

Policies for Maintaining Web Pages

Pages must relate to the Institute's mission.

Authors of official MCC and affiliated pages (not class-generated or personal) are required to announce their Web presence by sending an announcement to

webmaster@mccmulund.ac.in. Mails sent to this address will be placed in a MCC Public E-Mail Folder in the MCC's official web site.The announcement should include:

1. The URL.
2. A brief explanation of content or purpose of the pages (i.e., Web pages for an administrative or academic unit, etc.). The primary page must include a link to the MCC Home Page and, if applicable, contain additional links to the sponsoring organization or department.

5.6 Institute Database (of eGovernance) Use Policy

This Policy relates to the databases maintained by the Institute administration under the Institute's eGovernance.

Data is a vital and important Institute resource for providing useful information. Its use must be protected even when the data may not be confidential.

MCC has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the Institute's approach to both the access and use of this Institute resource.

A. **Database Ownership**: PTVA's Mulund College of Commerce Institute is the data owner of all the Institute's institutional data generated in the Institute.
B. **Custodians of Data**: Individual Sections or departments generate portions of data that constitute Institute's database. They may have custodianship responsibilities for portions of that data.
C. **Data Administrators**: Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.
D. **MIS Components**: For the purpose of eGovernance, Management Information

System requirements of the Institute may broadly be divided into seven categories. These are:

- MANPOWER INFORMATION MANAGEMENT SYSTEM (MIMS)
- STUDENTS INFORMATION MANAGEMENT SYSTEM (SIMS)
- FINANCIAL INFORMATION MANAGEMENT SYSTEM (FIMS)
- PHYSICAL RESOURCES INFORMATION MANAGEMENT SYSTEM (PRIMS)
- PROJECT INFORMATION MONITORING SYSTEM (PIMS)
- LIBRARY INFORMATION MANAGEMENT SYSTEM (LIMS)
- DOCUMENT MANAGEMENT AND INFORMATION RETRIEVAL SYSTEM (DMIRS)

Here are some general policy guidelines and parameters for Sections, departments and administrative unit data users:

1. The Institute's data policies do not allow the distribution of data that is identifiable to a person outside the Institute.
2. Data from the Institute's Database including data collected by departments or individual faculty and staff, is for internal Institute purposes only.
3. One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies, the Institute makes information and data available based on those responsibilities/rights.

4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office of the Institute Registrar.
5. Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the Institute and departments should never respond to requests, even with a subpoena.
6. All requests from law enforcement agencies are to be forwarded to the Office of the Institute Registrar for response. At no time may information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation or other purposes. This includes organizations and companies which may be acting as agents for the Institute or its departments.
7. Database users who repackage data for others in their unit must inform the recipients of the above data access issues.

Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to:

- Modifying/deleting the data items or software components by using illegal access methods. Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
- Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
- Trying to break security of the Database servers.

Such data tampering actions by Institute member or outside members will result in disciplinary action against the offender by the Institute authorities.

If the matter involves illegal action, law enforcement agencies may become involved.

5.7 Responsibilities of Internet Unit

A. Campus Network Backbone Operations

1. The campus network backbone and its active components are administered, maintained and controlled by INTERNET UNIT.

2. INTERNET UNIT operates the campus network backbone such that service levels are maintained as required by the Institute Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

B. Physical Demarcation of Campus Buildings' Network

1. Physical connectivity of campus buildings already connected to the campus network backbone is the responsibility of INTERNET UNIT.
2. Physical demarcation of newly constructed buildings to the "backbone" is the responsibility of INTERNET UNIT. It essentially means exactly at which location the fiber optic based backbone terminates in the building will be decided by the INTERNET UNIT. The manner in which the building is to be connected to the campus network backbone (whether the type of connectivity should be of fiber optic, wireless or any other media) is also the responsibility of INTERNET UNIT.
3. INTERNET UNIT will consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.
4. It is not the policy of the Institute to actively monitor Internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the Institute's Internet links.

C. Network Expansion

Major network expansion is also the responsibility of INTERNET UNIT. Every 3 to 5 years, INTERNET UNIT reviews the existing networking facilities, and need for possible expansion. Network expansion will be carried out by INTERNET UNIT when the Institute makes the necessary funds available.

D. Wireless Local Area Networks

1. Where access through Fiber Optic/UTP cables is not feasible, in such locations INTERNET UNIT considers providing network connection through wireless connectivity.
2. INTERNET UNIT is authorized to consider the applications of Sections, departments, or divisions for the use of radio spectrum from INTERNET UNIT prior to implementation of wireless local area networks.

3. INTERNET UNIT is authorized to restrict network access to the Sections, departments, or divisions through wireless local area networks either via authentication or MAC/IP address restrictions.

E. Electronic logs

Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.

F. Global Naming and IP Addressing

INTERNET UNIT is responsible to provide a consistent forum for the allocation of campus network services such as IP addressing and domain name services. INTERNET UNIT monitors the network to ensure that such services are used properly.

G. Providing Net Access IDs and email Accounts

INTERNET UNIT 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 Institute upon receiving the requests from the individuals on prescribed proforma.

H. Network Operation Center

INTERNET UNIT is responsible for the operation of a centralized Network Operation Control Center. The campus network and Internet facilities are available 24 hours a day, 7 days a week. All network failures and excess utilization are reported to the INTERNET UNIT technical staff for problem resolution .

Non-intrusive monitoring of campus-wide network traffic on routine basis will be conducted by the INTERNET UNIT. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, INTERNET UNIT will analyse the net traffic offending actions or equipment are identified and protective restrictions are applied until the condition has been rectified or the problem has been resolved. In this process, if need be, a report will be sent to higher authorities in case the offences are of very serious nature.

I. Network Policy and Technology Standards Implementation

INTERNET UNIT is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network backbone.

J. Receiving Complaints

INTERNET UNIT may receive complaints from COMPUTER CENTER, 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.

INTERNET UNIT may receive complaints from the users if any of the user is not able to access network due to a network related problem at the user end. Such complaints may be generally through phone call to INTERNET UNIT.

The designated person in INTERNET UNIT receives complaints from the users/COMPUTER CENTER and coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.

K. Scope of Service

INTERNET UNIT will be responsible only for solving the network related problems or services related to the network.

L. Disconnect Authorization

INTERNET UNIT 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. In the event of a situation where the normal flow of traffic is severely degraded by a Section, department, or division machine or network, INTERNET UNIT endeavors to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Section, department, or division is disconnected, INTERNET UNIT provides the conditions that must be met to be reconnected.

5.8 Responsibilities of Institute Computer Center

A. Maintenance of Computer Hardware & Peripherals

COMPUTER CENTER is responsible for maintenance of the Institute owned computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to this Cell.

B. Receiving Complaints

COMPUTER CENTER may receive complaints from INTERNET UNIT, 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/INTERNET UNIT 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 Institute 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 of the Institute, such incidents should be brought to the notice of the INTERNET UNIT and Institute authorities.

F. Reporting incidents related to Network Operations

When the network port of any particular computer system is turned off due to virus or related activity that is affecting the network performance, the same will be informed to the COMPUTER CENTER by INTERNET UNIT. After taking necessary corrective action COMPUTER CENTER or service engineers should inform INTERNET UNIT about the same, so that the port can be turned on by them.

G. Rebuilding the Computer System

When the service engineers reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was having earlier. Further, after installing the

OS all the patches/latest service pack should also be properly installed. In case of anti-virus software, service engineers should make sure that its latest engine and pattern files are also downloaded from the net.

Further, before reformatting the hard disk, dump of only the data files should be taken for restoring it back after proper re-installation. Under no circumstances, software files from the infected hard disk dump should be used to write it back on the formatted hard disk.

H. Coordination with INTERNET UNIT

Where there is an element of doubt as to a particular problem on the computer connected to the network is related to the network or the software installed or hardware malfunctioning,

COMPUTER CENTER/service engineer may coordinate with INTERNET UNIT staff to resolve the problem with joint effort. This task should not be left to the individual user.

5.8.1 Responsibilities of Department or Sections

A. User Account

Any Centre, department, or Section or other entity can connect to the Institute network using a legitimate user account (Net Access ID) for the purposes of verification of affiliation with the Institute. The user account will be provided by INTERNET UNIT, upon filling up the prescribed application form and submitting it to INTERNET UNIT.

Once a user account is allocated for accessing the Institute's computer systems, 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.

As a member of PTVA's Mulund College of Commerce Institute community, when using the Institute' network facilities and its user account, it becomes user's duty to respect the Institute's reputation in all his/her electronic dealings within as well as outside the Institute.

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

B. Logical Demarcation of Department/ Section/Division Networks

In some cases, Section, department or Division might have created a internal network with in their premises. In such cases, the Section, department, or division assumes responsibility for the network service that is provided on all such internal networks on the School, department or division side of the network backbone. The School, department, or division is also responsible for operating the networks on their side of

the network backbone in a manner that does not negatively impact other network segments that are connected to the network backbone.

Each Section, department, or division should identify at least one person as a Point of Contact and communicate it to INTERNET UNIT and COMPUTER CENTER so that INTERNET UNIT or COMPUTER CENTER can communicate with them directly in case of any network/system related problem at its end.

C. Supply of Information by Section, Department, or Division for Publishing on /updating the MCC Web Site

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

Hardcopy of such information duly signed by the competent authority at Section, Department, or Division level, along with a softcopy to be sent to the webmaster operating from INTERNET UNIT. This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by Section, Department, or Division.

Links to any web pages that have to be created for any specific purpose or event for any individual department or faculty can be provided by the webmaster upon receiving the written requests. If such web pages have to be directly added into the official web site of the Institute, necessary content pages (and images, if any) have to be provided by the respective department or individual in a format that is exactly compatible with the existing web design/format. Further, such requests along with the soft copy of the contents should be forwarded to the Director, INTERNET UNIT well in advance.

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

1. This policy applies, in its entirety, to school, department, or division wireless local area networks/broadband connectivity within the academic complex. In addition to the requirements of this policy, school, departments, or divisions must register each wireless access point with INTERNET UNIT including Point of Contact information.
2. Obtaining Broadband connections and using the computers alternatively on the broadband and the Institute campus-wide network is direct violation of the Institute's IT Policy, as Institute. IT Policy does not allow broadband connections within the academic complex.
3. School, departments, or divisions must secure permission for the use of radio spectrum from INTERNET UNIT prior to implementation of wireless local area networks.
4. 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.

5. As inter-building wireless networks are also governed by the Institute IT Policy, setting up of such wireless .networks should not be undertaken by the Schools/Centers without prior information to INTERNET UNIT.

E. Security

In connecting to the network backbone, a school, department, or division agrees to abide by this Network Usage Policy under the Institute IT Security Policy. Any network security incidents are resolved by coordination with a Point of Contact (POC) 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 Institute are the property of the Institute and are maintained by INTERNET UNIT.

Tampering of these items by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to,

- Removal of network inlet box.
- Removal of UTP cable from the room.
- Opening the rack and changing the connections of the ports either at jack panel level or switch level.
- Taking away the UPS or batteries from the switch room.
- Disturbing the existing network infrastructure as a part of renovation of the location INTERNET UNIT will not take any responsibility of getting them rectified and such tampering may result in disconnection of the network to that segment or the individual, until the compliance is met.

G. Additions to the Existing Network

Any addition to the existing network done by Section, department or individual user should strictly adhere to the Institute network policy and with prior permission from the competent authority and information to INTERNET UNIT.

Institute Network policy requires following procedures to be followed for any network expansions:

- All the internal network cabling should be as on date of CAT 6 UTP.
- UTP cabling should follow structured cabling standards. No loose and dangling UTP cables be drawn to connect to the network.
- UTP cables should be properly terminated at both ends following the structured cabling standards.
- Only managed switches should be used. Such management module should be web enabled. Using unmanaged switches is prohibited under Institute's IT policy. Managed switches give the facility of managing them through web so

that INTERNET UNIT can monitor the health of these switches from their location. However, the hardware maintenance of so expended network segment will be solely the responsibility of the department/individual member. In case of any network problem created by any computer in such network, if the offending computer system is not locatable due to the fact that it is behind an unmanaged hub/switch, the network connection to that hub/switch will be disconnected, till compliance is met by the user/department.

- As managed switches require IP address allocation, the same can be obtained from INTERNET UNIT on request.

H. Structured Cabling as a part of New Buildings

All the new buildings that will be constructed in the academic complex here onwards should have the structured cabling included in their building plans like any other wiring such as electrical and telephone cabling, for LAN as a part of the building layout Plan. Engineering Branch may make provisions in their designs for at least one network point in each room. All such network cabling should strictly adhere to the structured cabling standards used for Local Area Networks.

I. Campus Network Services Use Agreement

The “Campus Network Services Use Agreement” should be read by all members of the Institute who seek network access through the Institute campus network backbone. This can be found on the Intranet Channel of the Institute web site. All provisions of this policy are considered to be a part of the Agreement. Any Section, Department or Division or individual who is using the campus network facility , is considered to be accepting the Institute IT policy. It is user’s responsibility to be aware of the Institute IT policy. Ignorance of existence of Institute IT policy is not an excuse for any user’s infractions.

J.Enforcement

INTERNET UNIT periodically scans the Institute 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.

5.8.2 Responsibilities of the Administrative Units

INTERNET UNIT needs latest information from the different Administrative Units of the Institute for providing network and other IT facilities to the new members of the Institute and for withdrawal of these facilities from those who are leaving the Institute, and also for keeping the MCC web site up-to-date in respect of its contents.

- The information that is required could be broadly of the following nature:
- Information about New Appointments/Promotions.
- Information about Super annuations / Termination of Services.
- Information of New Enrolments.
- Information on Expiry of Studentship/Removal of Names from the Rolls.
- Any action by the Institute authorities that makes n individual ineligible for using the Institute’s network facilities.

- Information on Important Events/Developments/Achievements.
- Information on different Rules, Procedures, Facilities Information related items nos. A through E should reach Director (INTERNET UNIT) and Information related items nos. F and G should reach webmaster well in-time.

Hard copy of the information that is supplied by the concerned administrative unit duly signed by competent authority along with its soft copy (either on mobile storage devices or mobiles or PDA or by email) should be sent to INTERNET UNIT so as to reach the above designated persons.

5.8.3 Guidelines on Computer Naming Conventions

In order to troubleshoot network problems and provide timely service, it is vital to be able to quickly identify computers that are on the campus network. All computer names on the campus network must use the Institute standard conventions. Computers not following standard naming conventions may be removed from the network at the discretion of INTERNET UNIT.

All the computers should follow the standard naming convention.

Guidelines for running Application or Information Servers

Section/Departments may run an application or information server.

Individual faculty, staff or students on the MCC 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 MCC network.

Responsibilities for Those Running Application or Information Servers

Sections/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 MCC Guidelines for Web Presence.
2) Obtain an IP address from INTERNET UNIT to be used on the server
3) Get the hostname of the server entered in the DNS server for IP Address resolution.
4) Institute IT Policy's naming convention should be followed while giving the host names.
5) 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.
6) 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.
7) Operating System and the other security software should be periodically updated.
8) Sections/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 in writing to INTERNET UNIT on installing such Servers and obtain necessary IP address for this purpose.

For general information to help you decide whether or not to run a department or organization web server, contact the INTERNET UNIT.

Guidelines for hosting Web pages on the Internet/Intranet.

Mandatory:

1. Provide the full Internet e-mail address of the Web page maintainer.
2. Provide a link to the MCC home page from the parent (department of origin) home page.
3. Provide a link to the parent home page ("Return to department's home page") on all supporting local pages.
4. Maintain up to date pages. Proofread pages and test links before putting them on the Web, and regularly test and update links.
5. Know the function of HTML tags and use them appropriately.
6. Make provision for providing information without images as printer-friendly versions of the important web pages.

Recommended:

1. Provide information on timeliness (for example: August 2005; updated weekly; updated monthly, etc.).
2. Provide a section indicating "What's New."
3. Provide a caution statement if link will lead to large pages or images.
4. Indicate restricted access where appropriate.
5. Avoid browser-specific terminology.
6. Provide link text that is clear without the link saying 'click here' whenever hyperlinks are used.
7. Maintain visual consistency across related pages.
8. Provide a copyright statement (if and when appropriate).
9. Keep home pages short and simple.
10. Avoid using large graphics or too many graphics on a single page.
11. Provide navigational aids useful to your users (Link to Home, Table of Contents, Next Page, etc.).
12. Maintain links to mentioned pages.
13. Make your Web pages easy to maintain for yourself and anyone who might maintain them in the future.
14. Avoid active links to pages that are in development. Place test or draft pages in your "test," "temp," or "old" subdirectory. Remember that nothing is private on the Internet: unlinked pages in your directory may be visible.
15. Check your finished page with a variety of browsers, monitors, and from both network and modem access points. It is also recommended that you check your page with a Web validation service.

16. Think of your users--test with primary user groups (which will be mix of users linking through our high-speed network, and users linking via much slower modems).
17. Confirm to accepted, standard HTML codes.

Guidelines for Desktop Users

These guidelines are meant for all members of the MCC Network User Community and users of the Institute network.

1. Due to the increase in hacker activity on campus, Institute IT Policy has put together recommendations to strengthen desktop security. The following recommendations include:
2. 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.
3. 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.Whenever possible, security policies should be set at the server level and applied to the desktop machines.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.
4. The password should be difficult to break. Password, defined as:
   i. must be minimum of 6-8 characters in length
   ii. must include punctuation such as ! $ % & * , . ? + - =
   iii. must start and end with letters
   iv. must not include the characters # @ ' " `
   v. must be new, not used before
   vi. Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No.etc.
   vii. passwords should be changed periodically and also when suspected that it is known to others.
   viii. Never use ‘NOPASS’ as your password
   ix. Do not leave password blank and
   x. Make it a point to change default passwords given by the software at the time of installation
5. The password for the user login should follow the same parameters outlined above.
6. The guest account should be disabled.
7. New machines with Windows XP should activate the built-in firewall.
   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.

8. 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).
9. When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original CDs of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.
10. Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.
11. 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.
12. In addition to the above suggestions, INTERNET UNIT 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.
13. If a machine is compromised, INTERNET UNIT will shut the port off. This will isolate the computer, until it is repaired as per the guidelines. At that time, the port will be turned back on.
14. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, INTERNET UNIT technical personnel can scan the servers for vulnerabilities upon request.

5.9 Video Surveillance Policy

5.9.1 The system

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

1.2. 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.

1.3. 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 Cemera installation is in use.

1.4. 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.

5.9.2 Purpose of the system

1.5. The system has been installed by Institute 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:

- 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

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

5.9.3 Covert recording

Covert cameras may be used under the following circumstances on the written authorisation or request of the Senior officer, Registrar and where it has been assessed by the Head of Security and Facilities Services and the Data Protection Officer:

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- That there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.
- Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorised activity.
- The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

5.10 The Security Control Room

- Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.
- No unauthorised access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorised members of senior management, police officers and any other person with statutory powers of entry.
- Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorisation from the Registrar. In an emergency and where it is not reasonably practicable to secure prior

authorisation, access may be granted to persons with a legitimate reason to enter the Control Room.

- Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organisation they represent, the person who granted authorisation and the times of entry to and exit from the centre. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

5.11 Security Control Room Administration and Procedures

- Details of the administrative procedures which apply to the Control Room will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.
- Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

5.12 Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP Cemera images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Cemera.

5.13 Recording

- Digital recordings are made using digital video recorders operating in time lapse mode.
- Incidents may be recorded in real time.
- 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.
- All hard drives and recorders shall remain the property of Institute until disposal and destruction.

5.14 Access to images

- All access to images will be recorded in the Access Log as specified in the Procedures Manual
- Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.

5.15 Access to images by third parties

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.

5.16 Access to images by a subject

- CCTV/IP Camera 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 Camera 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.
- A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection Officer. Subject Access Request Forms are obtainable from the Security Office, between the hours of 1020 and 1400 and 1430 to 1800 Monday to Saturday (except Second and fourth Saturday), except when Institute is officially closed or from the Data Protection Officer, the Records Office during the same hours.
- The Data Protection Officer will then arrange for a copy of the data to be made and given to the applicant. The applicant must not ask another member of staff to show them the data, or ask anyone else for a copy of the data. All communications must go through the Institute Data Protection Officer. A response will be provided promptly and in any event within forty days of receiving the required fee and information.
- The Data Protection Act gives the Data Protection Officer 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.
- All such requests will be referred to the Security Control room Supervisor or by the Data Protection Officer.
- If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

5.17 Request to prevent processing

- 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.
- All such requests should be addressed in the first instance to the Security Control Room Supervisor or the Data Protection Officer, 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.

5.18 Complaints

- 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 the first instant to the Security Control Room supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Universities Centralised Complaints Procedure by obtaining and completing a Institute Complaints Form and a copy of the procedure. Complaints forms may be obtained from the Security Office, and the Registrar's Office. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Data Protection Officer, These rights do not alter the existing rights of members of Institute or others under any relevant grievance or disciplinary procedures.

5.19 Compliance monitoring

- The contact point for members of Institute or members of the public wishing to enquire about the system will be the Security Office which will be available during the hours of 1020 and 1400 and 1430 to 1800 Monday to Saturday (except second and fourth Saturday) except when Institute is officially closed.
- Upon request enquirers will be provided with:
- A summary of this statement of policy
- An access request form if required or requested
- A subject access request form if required or requested
- A copy of the Institute central complaints procedures

All documented procedures will be kept under review and a report periodically made to the Estates Management Committee. The effectiveness of the system in meeting its purposes will be kept under review and reports submitted as required to the Estates Management Committee.

3. Committees for policy implementation

This policy shall be revised and implemented by the committee formed annually.

4. Impact of the policy on processes

The policy would apply to:

- Stake holders on campus or off campus
- Students: UG, PG, Research
- Faculty
- Administrative Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests

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