Shoolini University

SHOOLINI
UNIVERSITY
SOLAN, HP

IT POLICY

www.shoolinuniversity.com

INDEX

7. Setting up of Wireless Local Area Networks/Broadband

7.1 Connectivity

7.2 Security

7.3 Preservation of Network Equipment and Accessories

7.4 Additions to the Existing Network

7.5 Structured Cabling as a part of New Buildings

7.6 Enforcement

8. Responsibilities of the Administrative Units

8.1 Guidelines on Computer Naming Conventions

8.2 School/Departments may run an application or information server.

8.3 Responsibilities for Those Running Application or Information Servers

8.4 Data Backup, Security, and Disclaimer

1. Introduction to Shoolini IT Policy

IT Policy for a University revolve along the following five pillars:

- Help Desk
- Application Development and implementation
- Network
- IT infrastructure & Maintenance
- Security and Redundancy

The IT Policy for Shoolini University is designed. Based upon above-mentioned five-pillars

1.1 Need for IT Policy

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

Undoubtedly, Intranet & Internet services have become the most important resources in educational institutions & research organizations. Realizing the importance of these services, Shoolini University took initiative way back in 2010 and established basic network infrastructure in the academic complex of the university.

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 university's academic environment.

IT DEPARTMENT that has been given the responsibility of running the university's intranet & Internet services.*IT DEPARTMENT* is running the Firewall security, Proxy, *DHCP, DNS,* email, web and application servers and managing the network of the university. We are getting its Internet bandwidth from JIO. Total bandwidth availability is 1Gbps (leased line). A sperate network is also established in the campus JIO which also gives a limited amount of free data to the users. To secure the network, the *IT DEPARTMENT* has been taking appropriate steps by installing firewalls, access controlling and installing virus checking and content filtering software at the gateway.

Policies also serve as blueprints that help the institution implement security measures. An effective security policy is as necessary to a good information security program as a solid foundation for the building. Hence, Shoolini University also is proposing to have its own *IT*

Policy that works as guidelines for using the university's computing facilities including computer hardware, software, email, information resources, intranet and Internet access facilities, collectively called "Information Technology (*IT*)". Hence, this document attempts to propose some *IT* policies and guidelines that would be relevant in the context of this university.

While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users. Information security in general and therefore policies that govern information security process are also dynamic. They need to be reviewed regularly and modified to reflect changing technology, changing requirements of the *IT* user community, and operating procedures.

Purpose of *IT* policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help organization, departments and individuals who are part of the university community to understand how University policy applies to some of the significant areas and to bring conformance with stated policies. *IT* policies may be classified into the following groups:

- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Web Site Hosting Policy
- University Database Use Policy

Further, the policies will be applicable at two levels:

- End Users Groups (Faculty, students, Senior administrators, Officers, and other staff)
- Network Administrators

It may be noted that university *IT* Policy applies to technology administered by the university centrally or by the individual departments, to information services provided by the university administration, or by the individual departments, or by individuals of the university community, or by the authorized resident or non-resident visitors on their hardware connected to the university network. This *IT* policy also applies to the resources administered by the central administrative departments such as Library, *IT DEPARTMENT*s, Laboratories, Offices of the university recognized Associations/Unions, or hostels and guest houses, or residences wherever the network facility was provided by the university.

Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the university *IT* policy. Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the University's information technology infrastructure, must comply with the Guidelines. Certain violations of *IT* policy

laid down by the university by any university member may even result in disciplinary action against the offender by the university authorities.

1.2 Applies to Stakeholders on-campus or off-campus

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

1.3 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

2. Section I: IT Hardware Installation Policy

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

2.1 Who is Primary User

An individual in whose room the computer is installed and is primarily used by him/her is “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.

2.2 What is End User Computer Systems?

Apart from the client PCs used by the users, the university will consider servers not directly administered by the *IT DEPARTMENT*, 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 *IT DEPARTMENT*, are still considered under this policy as "end- users" computers.

2.3 Warranty & Annual Maintenance Contract

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

2.4 Power and Power Backup Policy

The continued and uninterrupted operation of the Shoolini Computer Center and servers and network equipment housed in it is essential to the mission of the College. Director operations has installed a *160-KVA* diesel generator and all the labs have power system (*UPS*). The purpose of this policy is to set forth guidelines for the operation, testing, and maintenance of these systems.

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 a 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 the proper earthling and have properly laid electrical wiring.

2.5 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.

2.6 File and Print Sharing Facilities

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

2.7 Shifting Computer from One Location to another

A computer system may be moved from one location to another with a prior written intimation to the *IT DEPARTMENT*, as *IT DEPARTMENT* 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 *IT DEPARTMENT* 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 *IT DEPARTMENT* in writing/by email, the connection will be restored.

2.8 Maintenance of Computer Systems provided by the University

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

2.9 Noncompliance

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

2.10 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 and a copy of the notification will be sent to the *IT DEPARTMENT*, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The *IT DEPARTMENT* will guide as needed for the individual to gain compliance.

3. Section II: Software Installation and Licensing Policy

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

Respecting the anti-piracy laws of the country, University *IT* policy does not allow any pirated/unauthorized software installation on the university-owned computers and the computers connected to the university campus network. In case of any such instances, the university will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

3.1 Operating System and its Updating

- Individual users should make sure that respective computer systems have their *OS* updated in respective of their service packs/patches, through the Internet. This is particularly important for all *MS* Windows-based computers (both *PC*s and Servers). Updating *OS* by the users helps their computers in fixing bugs and vulnerabilities in

the *OS* that was 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.

- University as a policy encourages user community to go for open-source software such as Linux, Open office to be used on their systems wherever possible.

3.2 Antivirus Policy

Computer systems used in the university should have anti-virus software installed as a university have office 365 tie-up with Microsoft, which Windows Defender installed with the operating system and it should always be active on each server or computer system. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy. 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.

3.3 Backups Data Policy

Each Department Head to indicate the list of stand-alone systems and categorise these as either

- Not Critical
- Critical

Based on assessment whether the data is critical to the functioning of the university or department. If data is not critical, in that case, it is the responsibility of User to ensure weekly back-up of the stand-alone system in the common drive allocated to the user in the Labs. *IT DEPARTMENT* will ensure backup of stand-alone systems every week in coordination with the concerned faculty/staff. A *LAN* backup system is implemented for this in critical areas.

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.

3.4 Noncompliance

University faculty, staff and students not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files inoperable computer resulting in loss of productivity risk of spread of infection to others confidential data being revealed to unauthorized persons an individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even whole university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

4. Section III: Cyber Security Policy

Network connectivity provided through the University referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (*VPN*) connection, is governed under the University *IT* Policy. The Communication & Information Services (*IT DEPARTMENT*) is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to *IT DEPARTMENT*.

4.1 IP Address Allocation

Any computer (*PC*/Server) that will be connected to the university network, should have an IP-address assigned by the *IT DEPARTMENT*. 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 IP address allocation and fill it up and get the *IP* address from the *IT DEPARTMENT*.

An *IP* address allocated for a 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. The *IP* address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

4.2 DHCP and Proxy Configuration by Individual Departments /Sections/ Users

Use of any computer at the 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 an absolute violation of *IP* address allocation policy of the university. Similarly, the configuration of proxy servers should also be avoided, as it may interfere with the service run by *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. The connection will be restored after receiving written assurance of compliance from the concerned department/user.

4.3 Running Network Services on the Servers

Individual departments/individuals connecting to the university network over the *LAN* may run server software, e.g., *HTTP*/Web server, *SMTP* server, *FTP* server, only after bringing it to the knowledge of the *IT DEPARTMENT* in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university 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 University's network connection must comply with all policies and rules of those networks. This applies to all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes. Network traffic will be monitored for security and performance reasons at *IT DEPARTMENT*. 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.

4.4 Dial-up/Broadband Connections

Computer systems that are part of the University's campus-wide network, whether university's property or personal property, should not be used for dial-up/broadband connections, as it violates the university'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.

4.5 Wireless Local Area Networks

- 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 *IT DEPARTMENT* including Point of Contact information.

- School, departments, or divisions must inform *IT DEPARTMENT* for the use of radio spectrum before the implementation of wireless local area networks.
- 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.
- If individual School wants to have an inter-building wireless network, before installation of such a network, it should obtain permission from the university authorities whose application may be routed through the Coordinator, *IT DEPARTMENT*.

5. Section IV: Email Account Use Policy

To increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and academic & other official purposes. E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc.

To receive these notices, the e-mail address must be kept active by using it regularly. Staff and faculty may use the email facility by logging on to https://mail.shooliniuniversity.com with their User *ID* and password. For obtaining the university's email account, the user may contact the *IT DEPARTMENT* for an email account and default password by applying a prescribed proforma.

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

- The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- Using the facility for illegal/commercial purposes is a direct violation of the university's *IT* policy and may entail the 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 a generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
- While sending large attachments to others, a user should make sure that the recipient has an email facility that allows him to receive such large attachments.

- User should keep the mailbox used space within about 80% usage threshold, as ‘mailbox full’ or ‘mailbox all fullest’ situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
- User should not open any mail or attachment that is from an unknown and suspicious source. Even if it is from a known source, and if it contains any attachment that is suspicious or looks dubious, a 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 the potential to damage the valuable information on your computer.
- Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use permanently 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 the user’s responsibility to keep a backup of the incoming and outgoing mails of their account.
- User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
- User should refrain from intercepting or trying to break into others email accounts, as it is infringing the privacy of other users.
- While using the computers that are shared by other users as well, any email account that was accidentally left open by another user should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
- Impersonating email account of others will be taken as a serious offence under the university *IT* security policy.
- It is ultimately everyone’s responsibility to keep their e-mail account free from violations of the university’s email usage policy.

The above laid down policies 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 university’s campus network, or by using the resources provided by the university to the individual for official use even from outside.

6. Section V: Data Privacy Policy

This Policy relates to the databases maintained by the university administration under the university’s governance. Data is a vital and important University resource for providing useful information. Its use must be protected even when the data may not be confidential. *SU* has its policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the university's approach to both the access and use of this university resource.

- Database Ownership: Shoolini University is the data owner of all the University's institutional data generated in the university.

- Custodians of Data: Individual Sections or departments generate portions of data that constitute the University's database. They may have custodianship responsibilities for portions of that data.
- Data Administrators: Data administration activities outlined may be delegated to some of the officers in that department by the Data Custodian.
- *MIS* Components: For eGovernance, Management Information System requirements of the university 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:

- The university's data policies do not allow the distribution of data that is identifiable to a person outside the university.
- Data from the University's Database including data collected by departments or individual faculty and staff is for internal university purposes only.
- 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 university makes information and data available based on those responsibilities/rights.
- 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 University Registrar.
- Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the University and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office of the University Registrar for the 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 university or its departments.
- All reports for *UGC*, *MHRD* and other government agencies will be prepared/compiled and submitted by the Registrar, Director *BCUD*, Controller of Examinations and Finance officer of the University.

- 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 the security of the Database servers.

Such data tampering actions by university member or outside members will result in disciplinary action against the offender by the university authorities. If the matter involves illegal activities, law enforcement.

6.1 Responsibilities of the University *IT DEPARTMENT*

- Maintenance of Computer Hardware & Peripherals: *IT DEPARTMENT* is responsible for maintenance of the university-owned computer systems and peripherals that are either under warranty or an annual maintenance contract and whose responsibility has officially been entrusted to this Cell.
- Receiving Complaints: *IT DEPARTMENT* may receive complaints from *IT DEPARTMENT* if any of the computer systems are causing network-related problems. *IT DEPARTMENT* 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 *IT DEPARTMENT* receives complaints from the users/*IT DEPARTMENT* 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.
- Scope of Service: *IT DEPARTMENT* 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.
- Installation of Un-Authorized Software: *IT DEPARTMENT* 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.
- 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 university, such incidents should be brought to the notice of the *IT DEPARTMENT* and university authorities.

- 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 *IT DEPARTMENT* by INTERNET UNIT. After taking necessary corrective action *IT DEPARTMENT* or service engineers should inform *IT DEPARTMENT* about the same so that the port can be turned on by them.
- 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 the 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 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.
- Coordination with *IT DEPARTMENT*: 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, a service engineer may coordinate with *IT DEPARTMENT* staff to resolve the problem with a joint effort. This task should not be left to the individual user.

7. Setting up of Wireless Local Area Networks/Broadband

7.1 Connectivity

- 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 *IT DEPARTMENT* including Point of Contact information.
- Obtaining Broadband connections and using the computers alternatively on the broadband and the university campus-wide network is direct violation of the university's *IT* Policy, as university. *IT* Policy does not allow broadband connections within the academic complex.
- School, departments, or divisions must secure permission for the use of radio spectrum from *IT DEPARTMENT* prior to implementation of wireless local area networks.
- 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.
- As inter-building wireless networks are also governed by the University *IT* Policy, setting up of such wireless networks should not be undertaken by the Schools/Centers without prior information to *IT DEPARTMENT*.

7.2 Security

In connecting to the network backbone, a school, department, or division agrees to abide by this Network Usage Policy under the University *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*.

7.3 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 *IT DEPARTMENT*. 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 *IT DEPARTMENT* 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.

7.4 Additions to the Existing Network

Any addition to the existing network done by Section, department or individual user should strictly adhere to the university network policy and with prior permission from the competent authority and information to *IT DEPARTMENT*.

University 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 are 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 the university's *IT* policy. Managed switches give the facility of managing them through the

web so that *IT DEPARTMENT* 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 since 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 *IT DEPARTMENT* on request.

7.5 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.

7.6 Enforcement

IT DEPARTMENT periodically scans the University 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.

8. Responsibilities of the Administrative Units

IT DEPARTMENT needs latest information from the different Administrative Units of the University for providing network and other *IT* facilities to the new members of the university and for withdrawal of these facilities from those who are leaving the university, and also for keeping the *SU* 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 annotations / Termination of Services.
- Information of New Enrolments.
- Information on Expiry of Studentship/Removal of Names from the Rolls.
- Any action by the university authorities that makes individual ineligible for using the university'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 (*IT DEPARTMENT*) 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 *IT DEPARTMENT* so as to reach the above designated persons.

8.1 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 University standard conventions. Computers not following standard Running Application or Information Servers

8.2 School/Departments may run an application or information server.

Individual faculty, staff or students on the *SU* 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 *SU* network.

8.3 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.
- Application or information server content and services must follow content guidelines as described in SU Guidelines for Web Presence.
- Obtain an IP address from *IT DEPARTMENT* to be used on the server
- Get the hostname of the server entered in the *DNS* server for *IP* Address resolution. University IT Policy's naming convention should be followed while giving the hostnames.
- 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.
- 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.
- Operating System and the other security software should be periodically updated.
- Sections/Departments may run an application or information server provided they do the following:
  - Provide their computer, software, and support staff
  - Provide prior information in writing to *IT DEPARTMENT* on installing such Servers and obtain the necessary IP address for this purpose.
  - For general information to help you decide whether to run a department or organization web server, contact the *IT DEPARTMENT*.

8.4 Data Backup, Security, and Disclaimer

IT DEPARTMENT will not be liable for the loss or corruption of data on the individual user's computer as a result of the use and/or misuse of his/her computing resources (hardware or software) by the user or from any damage that may result from the advice or actions of an *IT DEPARTMENT* staff member in the process of helping the user in resolving their network/computer-related problems. Although *IT DEPARTMENT* makes a reasonable attempt to provide data integrity, security, and privacy, the User accepts full responsibility for backing up files in the assigned Net Access *ID*, storage space or email Account. Also, *IT DEPARTMENT* makes no guarantee concerning the security or privacy of a User's electronic messages.

The User agrees to be held liable for the improper use of equipment or software, including copyright violations and agrees to defend, indemnify and hold *INTERNET UNIT* or *COMPUTER CENTER*, as part of *SUK*, harmless for any such liability or expenses. *SUK* retains the right to change and update these policies as required without notification to the User.