MAR ATHANASIOS COLLEGE FOR ADVANCED STUDIES TIRUVALLA

(MACFAST)

MACFAST™

Igniting wisdom since 2001

IT POLICY

IT POLICY

Introduction

The IT policy of the college is framed to maintain, secure, appropriate, and legal use of Information Technology (IT) infrastructure established on the campus. The policy provides guidelines on the use of IT resources of the college which include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

Systems & IT wing is vested with the responsibility of running the intranet and Internet services. The wing is administering the Firewall security, Proxy, DHCP, DNS, Email, Web, and Application Servers and manages the network of the college which includes access controls and installing virus checking and content filtering at the gateway.

This document proposes a set of policies and guidelines which need to be reviewed on a regular basis and modified to reflect changing technology and requirements of the IT user community, and operating procedures.

Subdivisions of IT policy

IT policy of the college has been framed with the following subdivisions.

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

The policy shall be applicable at two levels:

1. End Users Groups (Faculty, students, senior administrators, Officers and other staff)
2. Network Administrators

This policy applies to the resources administered by the central administrative departments such as Library, Computer Labs, Laboratories, Administrative offices of the college. The guidelines given in this policy is applicable to all the faculty, students, staff, departments, authorised visitors/visiting faculty, and others who may be granted permission to use the information technology infrastructure of the

college. Violations of IT policy may even result in disciplinary action against the offender/s by the college authorities. If the matter requires the involvement of legal action, law enforcement agencies may also be informed.

Hardware Installation Policy

The network users of the college need to observe certain precautions while getting their computer hardware or peripherals installed so that they may face minimum inconvenience of interruptions due to hardware failures. The policy deals with the following.

A. Primary User

An individual in whose room the computer is installed and is used primarily by him/her is the "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. End User of Computer Systems

Apart from the client PCs, the college will consider servers not directly administered by Systems & IT, 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 Systems & IT, are still considered under this policy as "end-users" computers.

C. Warranty and Annual Maintenance Contract

Computers purchased by any Section/Department/Project Investigator 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 reinstallation and checking virus related problems also and should be monitored for the proper and timely maintenance.

D. Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS if available. 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 earthing 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 might 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 the network, they should be protected with password 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 Systems & IT, as it maintains a record of computer identification names (MAC Address, and Serial Number) and corresponding IP address. Such computer identification names follow the convention that comprises the Department name abbreviation and serial number. As and when any deviation is found for any computer system, network connection would be disabled and the same will be informed to the user via email/phone, if the user is identified. When the end user meets the compliance and informs the Systems & IT in writing/by email, connection will be restored.

H. Maintenance of Computer Systems

For all the computers that are purchased by the college, SYSTEMS & IT wing of the college will attend to the complaints related to any maintenance related problems.

I. Noncompliance

Faculty, staff, and students of the college, who do not comply 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 and inoperable computers, resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, or even whole departments. Hence it is critical to bring all computers into compliance as soon as they are recognized as non-compliant.

J. SYSTEMS & IT Wing Interface

Upon finding a non-compliant computer affecting the network Systems & IT wing 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 SYSTEMS & IT wing, if applicable. The individual users will follow-up the notification to be certain that his/her computer gains necessary compliance. The SYSTEMS & IT wing shall provide guidance as needed for the individual to gain compliance.

Software Installation and Licensing Policy

Purchase of computers by the individual sections/departments/project investigator should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed. The IT policy of the college does not allow pirated /unauthorized software installation on

the computers owned by the college and the computers connected to the campus network. In case of any such instance, the department/individual shall personally be responsible for the use of any pirated software.

A. Operating System and its Updating

1. Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through the 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 are 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. The college has made it as a policy to encourage its user community to go for open-source software such as Linux, Open office to be used on their systems wherever possible.
3. Any MS Windows OS based computer that is connected to the network should access http://windowsupdate.microsoft.com website 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 the users' responsibility to make sure that the updates are being done properly.

B. Antivirus Software and its Updating

1. Computer systems used in the college should have anti-virus software / Microsoft DEFENDER antivirus installed, and it should be always active. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.
2. Individual users should make sure that respective computer systems have current virus protection software installed and maintained. He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's technical skills, the end-user is responsible for seeking assistance from any service-providing agency.

C. Backups of Data

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. Preferably, at the time of OS installation itself, one can have the computer’s hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user’s data files on the D drive. Apart from this,

users should keep their valuable data either on an external storage device or Google Drive for data integration.

D. Noncompliance

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

E. SYSTEMS & IT WING Interface

Upon finding a non-compliant computer, the SYSTEMS & IT wing will notify the individual responsible for the system and bring it into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the SYSTEMS & IT wing, if applicable. The individual user shall follow-up the notification to be certain that his/her computer gains necessary compliance. The SYSTEMS & IT wing will provide guidance as needed for the individual to gain compliance.

Network (Intranet and Internet) Use Policy

Network connectivity provided through the College, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the College IT Policy. The SYSTEMS & IT wing is responsible for the on-going maintenance and support of the Network, exclusive of local applications. Problems within the network should be reported to SYSTEMS & IT wing.

A. IP Address Allocation

Any computer (PC/Server) that will be connected to the network, should have an IP address assigned by the SYSTEMS & IT wing. Following a systematic approach, the range of IP addresses that will be allocated to each group is decided. So, any computer connected to the network from that group will be allocated an IP address only from that Address pool. Further, each network port in the room from where that computer is connected will have binding internally with that IP address so that no other person uses that IP address unauthorised 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 SYSTEMS & IT wing. 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 Department /Section/ User

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 college. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by SYSTEMS & IT wing. 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 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 SYSTEMS & IT wing in writing and after meeting the requirements of the college IT policy for running such services. Non-compliance with this policy is a direct violation of the college IT policy and will result in termination of their connection to the Network. SYSTEMS & IT wing takes no responsibility for the content of machines connected to the Network, regardless of whether those machines belong to the college or individuals. SYSTEMS & IT wing 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 college network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the College Network connects. College 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 SYSTEMS & IT wing. Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection.

D. Dial-up/Broadband Connections

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

This policy applies, in its entirety, to the department, or division of wireless local area networks. In addition to the requirements of this policy departments, or divisions must register each wireless access point with SYSTEMS & IT wing including Point of Contact information.

Departments must inform SYSTEMS & IT wing for the use of radio spectrum, prior to implementation of wireless local area networks

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.

F. Internet Bandwidth obtained by Special Divisions

Internet bandwidth acquired by any department of the college under any research programme /project should ideally be pooled with the college's Internet bandwidth, and be treated as the common resource of the college. Under particular circumstances, which prevent any such pooling with the college Internet bandwidth, such networks should be totally separated from the campus network. All the computer systems using that network should have a separate IP address scheme (private as well as public) and the college gateway should not be specified as an alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the college 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 SYSTEMS & IT wing.

Non-compliance to this policy will be a direct violation of the college IT security policy.

Email Account Use Policy

To increase the efficient distribution of critical information to all faculty, staff and students, and the college administrators, it is recommended to utilize the college email services, for formal communication and for academic and other official purposes. Email for formal communications will facilitate the delivery of messages

and documents to campus and extended communities or to distinct user groups and individuals. Formal communications are official notices from the college to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general messages, official announcements, etc. To receive these notices, it is essential that the email address be kept active by using it regularly. For obtaining the college's email account, the user may contact SYSTEMS & IT wing for email account and default password by applying 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 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 almost 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.
6. 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. 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 onto 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 college IT security policy.
11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of college's email usage policy.
12. Any Spam mail received by the user into INBOX should be forwarded to admin@macfast.ac.in (students) or admin@macfast.org (faculty)
13. 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 admin@macfast.ac.in (students) or admin@macfast.org (faculty) for necessary action to delete from the spam mail category. It is recommended to empty this folder as frequently as possible.
14. While every effort is made to insure the privacy of the email users in the college community, this may not always be possible. Since employees are granted use of electronic information systems and network services to conduct their official duties, there may be instances when the College, based on approval from authorized officers, reserves and retains the right to access and inspect stored information without the consent of the user.

Web Site Hosting Policy

Official Pages

Sections, departments, and Associations of Teachers/Employees/Students may have pages on the official Web page of the college (www.macfast.org). Official Web pages must conform to the college Web Site Creation Guidelines for Web site hosting. As on date, the college webmaster is responsible for maintaining the official web site of the college viz., https://www.macfast.org only.

Personal Pages

The College official website provides space for the creation of profile for all faculty members under their respective department. It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal pages linked to the official website of the college that he/she wants to be added in the official website of the college. 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 institution.

Responsibilities for Those Maintaining Web Pages

Sections, departments, units, and individuals are responsible for maintaining their own Web pages. The Web pages (including personal pages) in the college website must adhere to the college Web Page Standards and Design Guidelines and should be approved by the Public Relations Team of the college.

Policies for Maintaining Web Pages

Pages must relate to the mission of the college. Authors of official site of the college and affiliated pages (not class-generated or personal) are required to announce their Web presence by sending an announcement to website@macfast.org.

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 college website Home Page and, if applicable, contain additional links to the sponsoring organization or department.

College Database (of e-Governance) Use Policy

This Policy relates to the databases maintained by the college administration under the college's e-Governance. Data is a vital and important resource for providing useful information. Its use must be protected even when the data may not be confidential. The college has its own policies regarding the creation of databases and access to information as well as a more generic policy on data access. Combined, these policies outline the college's approach to both the access and use of this college resource.

A. Database Ownership

The College is the data owner of all the college's institutional data generated in the campus.

B. Custodians of Data

Individual Sections or departments generate portions of data that constitute the college'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

Data pertaining to the crucial information collected as part of the functionalities provided by the MIS software developed by the college named as MACFAST Information System (www.macfastmis.org).

General guidelines and parameters for data users are as given below:

1. The college's data policies do not allow the distribution of data that is identifiable to a person outside the college.
2. Data from the College's Database including data collected by departments or individual faculty and staff, is for internal use of the college only.
3. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies. All such requests are to be forwarded to the Office of the Administrator.
4. Requests for information from any courts, attorneys, law enforcement agencies etc. shall be forwarded and handled by the Office of the Administrator.
5. At no time any information, including that identified as 'Directory Information', be released to outside entity for commercial, marketing, solicitation, or other purposes.
6. All reports for UGC, MHRD and other government agencies shall be prepared/compiled and submitted by the IQAC Coordinator of the College.
7. Tampering with 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 a member of the college or outside members will result in disciplinary action against the offender by the college authorities. If the matter involves illegal action, law enforcement agencies will become involved.

RESPONSIBILITIES OF SYSEMS & IT WING - NETWORKING

A. Campus Network Backbone Operations

The campus network backbone and its active components are administered, maintained and controlled by SYSTEMS & IT WING.

SYSTEMS & IT WING operates the campus network backbone which are maintained as required by the College Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

B. Physical Demarcation of Campus Buildings' Network

- Physical connectivity of campus buildings already connected to the campus network backbone shall be the responsibility of SYSTEMS & IT WING.
- Physical demarcation of newly constructed buildings to the "backbone" shall be the responsibility of SYSTEMS & IT wing. It essentially means exactly at which location the fibre optic-based backbone terminates in the buildings will be decided by the SYSTEMS & IT wing. The way the building is to be connected to the campus network backbone (whether the type of connectivity should be of fibre optic, wireless or any other media) is also the responsibility of SYSTEMS & IT wing.
- SYSTEMS & IT WING shall consult with the client(s) to ensure that end-user requirements are being met while protecting the integrity of the campus network backbone.
- Though the college is not actively monitoring Internet activity on the network, sometimes it becomes necessary to examine such activity when a problem has occurred or when optimizing traffic on the College's Internet links.

C. Network Expansion

Major network expansion is also the responsibility of SYSTEMS & IT wing. Every year, SYSTEMS & IT WING reviews the existing networking facilities, and need for possible expansion. Network expansion will be carried out by SYSTEMS & IT WING when the college makes the necessary funds available.

D. Wireless Local Area Networks

- Where access through Fiber Optic/UTP cables is not feasible, in such locations SYSTEMS & IT WING considers in providing network connection through wireless connectivity.
- SYSTEMS & IT WING is authorized to consider the applications of departments or divisions for the use of radio spectrum from SYSTEMS & IT WING prior to implementation of wireless local area networks.
- SYSTEMS & IT WING 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.
- SYSTEMS & IT WING is authorized to restrict network access through login ID and Password SYSTEMS & IT WING is authorized to monitor the

internet speed and other service conditions offered by the service provider.

E. Electronic logs

Electronic logs that are created as a part 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 & IP Addressing

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

G. Providing Net Access IDs

SYSTEMS & IT WING provides Net Access IDs to the individual users to enable them to use the campus-wide network and email facilities provided by the college upon receiving the requests from the individuals on prescribed proforma.

H. Network Operation Centre

SYSTEMS & IT WING is responsible for the operation of a centralized Network Operation Control Centre. 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 SYSTEMS & IT WING technical staff for problem resolution. Non-intrusive monitoring of campus-wide network traffic on routine basis will be conducted by the SYSTEMS & IT WING. If traffic patterns suggest that system or network security, integrity or network performance has been compromised, SYSTEMS & IT WING 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 necessary, a report will be sent to higher authorities in case the offences are of very serious nature.

I. Network Policy and Technology Standards Implementation

SYSTEMS & IT WING 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. Scope of Service

SYSTEMS & IT WING will be responsible only for solving the network related problems or services related to the network.

K. Disconnect Authorization

SYSTEMS & IT WING 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, SYSTEMS & IT WING endeavours 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, SYSTEMS & IT WING provides the conditions that must be met to be reconnected.

RESPONSIBILITIES OF SYSTEMS & IT WING – MAINTENANCE

A. Maintenance of Computer Hardware & Peripherals

SYSTEMS & IT Wing is responsible for maintenance of the college owned computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to this wing.

B. Receiving Complaints

SYSTEMS & IT Wing may receive complaints from the users. The designated person in the wing troubleshoots the complaints and contact with the service engineers of the respective brands of the computer systems to resolve the problem within a reasonable time limit, if necessary.

C. Scope of Service

SYSTEMS & IT Wing will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the college and was loaded by the company.

D. Installation of Unauthorised Software

SYSTEMS & IT Wing 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 SYSTEMS & IT Wing or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the college, such incidents should be brought to the notice of the SYSTEMS & IT WING and college authorities.

F. Reporting incidents related to Network Operations

When the network port of any computer system is turned off due to virus or related activity that is affecting the network performance, the same shall be informed to the SYSTEMS & IT wing. After taking necessary corrective action the port can be turned on by them.

G. Rebuilding the Computer System

When the IT Technician/Network Administrator 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.

RESPONSIBILITIES OF DEPARTMENT OR SECTIONS

A. User Account

Any Centre, department, or Section or other entity can connect to the College network using a legitimate user account (Net Access ID) for the purposes of verification of affiliation with the college. The user account will be provided by SYSTEMS & IT wing. Once a user account is allocated for accessing the college's computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the college 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 unauthorised use of their user account by others. As a member of the college community, when using the college network facilities and its user account, it becomes the user's duty to respect the College's reputation in all his/her electronic dealings within as well as outside the College.

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

B. Logical Demarcation of Department/ Section Networks

In some cases, Section, Department or Division might have created an internal network within 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 department or division side of the network backbone.

C. Supply of Information by Section, Department, or Division for Publishing on or updating the College Website

All Departments or Sections should provide updated information concerning them periodically. Hard copy of such information duly signed by the

competent authority at Section, Department, or level, along with a softcopy to be sent to the webmaster operating from SYSTEMS & IT WING. This policy is applicable even for advertisements notifications published in newspapers, and the events organized by Section or Department. Links to any web pages that shall 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.

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

1. This policy applies, in its entirety, department, or division wireless local area networks/ broadband connectivity within the academic complex. In addition to the requirements of this policy, departments, or sections must register each wireless access point with SYSTEMS & IT WING including Point of Contact information.
2. Obtaining Broadband connections and for using the personal computers/ laptops should authenticate from the SYSTEMS & IT wing
3. Departments, or Sections must secure permission for the use of radio spectrum from SYSTEMS & IT WING prior to implementation of wireless local area networks.
4. Departments, or Sections 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 coming under the College IT Policy, setting up of such wireless networks should not be undertaken by the Departments/Centres without prior information to SYSTEMS & IT WING.

E. Security

In connecting to the network backbone, department, or section agrees to abide by this Network Usage Policy under the College 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, Fibre optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries that are installed at different locations by the college are the property of the college and are maintained by SYSTEMS & IT WING. 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 SYSTEMS & IT WING 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 college network policy and with prior permission from the competent authority and information to SYSTEMS & IT wing. College 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. Using unmanaged switches is prohibited under the IT policy of the college. Managed switches give the facility of managing them through the web so that SYSTEMS & IT wing can monitor the health of these switches from their location.
- As managed switches require IP address allocation, the same can be obtained from SYSTEMS & IT wing 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. The team led by Estate Officer 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

All provisions of this policy are part of the Campus Network Services Use Agreement. Any Section, Department or Section or individual who is using the campus network facility, is accepting the college IT policy. It is the user's responsibility to be aware of the College IT policy. Ignorance about this policy is not an excuse for any user’s infractions.

J. Enforcement

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

RESPONSIBILITIES OF THE ADMINISTRATIVE UNITS

The respective administrative units shall be responsible to provide up to date information to the SYSTEMS & IT wing of the college. The information that is to be provided are the following:

- New Appointments/Promotions of staff members
- Superannuation/Termination of Services.
- New Enrolment of students
- Expiry of Studentship/Removal of Names from the Rolls.
- Any action by the college authorities that makes an individual ineligible for using the college's network facilities.
- Important Events/Developments/Achievements.

Hard copy of the information that is supplied by the concerned administrative unit duly signed by competent authority along with its soft copy shall be sent to SYSTEMS & IT wing.

Guidelines on Computer Naming Conventions

1. 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 College standard conventions. Computers not following standard naming conventions may be removed from the network at the discretion of SYSTEMS & IT wing.
2. All the computers should follow the standard naming convention
3. Computer name will be in the combination of a serial number + Department Name + MAC Address

Guidelines for running Application or Information Servers

1. Section/Departments may run an application or information server.
2. Individual faculty, staff or students 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 college network.

Guidelines for Desktop Users

Considering the possibility of hacker activity on campus, the following are put forward as a policy matter:

1. All desktop computers should have the latest version of antivirus and should regularly update latest virus definitions from the central server.
2. When a desktop computer is installed, all operating system updates and patches should be applied and monitored regularly. The policy recommends running the same once a week cycle for each machine.
3. All OS 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:
   - Must be minimum of 6-8 characters in length
   - Must include punctuation such as! $ % & * , . ? + - =
   - Must start and end with letters
   - Must not include the characters # @ ' " `
   - Must be new, not used before
   - Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No.etc.
   - Passwords should be changed periodically and also when suspected that it is known to others.
   - Do not leave password blank and 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 should activate the built-in firewall.
8. 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.
9. 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). 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. The policy recommends a regular backup strategy of backing up data on a regular basis (daily and/or weekly).

Video Surveillance Policy (CCTV)

1. **The System**

1.1 The system comprises: Fixed position bullet cameras & dome cameras; Monitors; NVRs; SSD Storages; 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 Camera 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.

2. **Purpose of the system**

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

a) Deter those having criminal intent
b) Assist in the prevention and detection of crime
c) Facilitate the identification, apprehension, and prosecution of offenders in relation to crime and public order.
d) 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.

The system shall 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

2.2 Covert recording

2.2.1 Covert cameras may be used with the written authorisation of the Administrator when there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place or where strict monitoring is required

2.2.2 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.

3. The Data Centre

3.1 Images captured by the system will be monitored and recorded in the SYSTEMS & IT, twenty-four hours a day. Monitors are not visible from outside the control room. Principal's office has also been provided with a LCD panel to monitor the same.

3.2 No unauthorised access to the Data Centre inside Rack 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, with the permission of the Principal.

3.3 Staff, students and visitors may be granted access to the Data Centre on a case-by-case basis and only then on written authorisation from the Principal of the College. 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 Data Centre.

3.4 Before allowing access to the Data Centre, 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.

4. Data Centre Administration and Procedures

4.1 Details of the administrative procedures which apply to the Data Centre 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.

4.2 Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Data Centre in charge is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict adherence to this policy and the procedures set out in the Procedures Manual.

5. All staff working in the Data Centre will be made aware of the sensitivity of handling CCTV/IP Camera images and recordings. The Data Centre in charge 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 Camera.

6. Recording

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

6.2 Images will normally be retained for fifteen days from the date of recording, and then automatically overwritten 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.

6.3 All hard drives and recorders shall remain the property of college until disposal and destruction.

7. Access to images

7.1 All access to images will be recorded in the Access Log as specified in the Procedures Manual

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

7.3 Access to images by third parties

7.3.1 Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

7.4 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.

7.4.1 A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Administrator. Subject Access Request Forms are obtainable from the Office.

7.4.2 The Administrator 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 college Administrator. A response will be provided promptly and in any event within forty days of receiving the required fee and information.

7.4.3 The Data Protection Act gives the Administrator 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.

7.4.4 All such requests will be referred to the Data Centre in charge or by the Administrator.

7.4.5 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 reason.

8. Request to prevent processing

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

8.2 All such requests should be addressed in the first instance to the Administrator, 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.

Policy for online delivery of classes

1. Zoom is the authorized / accepted platform for delivering all virtual classes.
2. Students are given with the link to enter Zoom based on the list received from the Academic offices.
3. Faculty are given privilege to create groups and enrol the students in their classes.
4. Class schedules must be done by the respective faculty/department.
5. Teachers will take the Attendance and could mark it in ERP also Assignments & Quizzes can be delivered via Google Classrooms/Moodle Platform
6. Recording of classes will be done only by the faculty
7. Recorded classes are made available to the students, if the student misses the class due to network/ power failure he/she will be authorized to view the recordings.

Policy for conducting Online Meetings

Any Department / Office who needs online meeting facility need to send a request to SYSTEMS & IT wing well in advance to schedule the meeting and to facilitate online meetings. However, on demand request is also accepted based on the availability of slots. The meetings are facilitated through Zoom / Google Meet

Policy for conducting Conference / Workshops for Larger Audience

Departments/Sections are encouraged to use Zoom integrated with YouTube and Facebook to reach the larger audience. A formal official email communication will be sent to SYSTEMS & IT wing to facilitate it with the approval of Deans / Directors / HODs / Section Heads.