Al-Ameen COLLEGE

Affiliated to Mahatma Gandhi University, Kottayam

IT POLICY 2020

TABLE OF CONTENTS

Introduction

Information Technology lays a significant role in the success of every academic institution. An IT security policy identifies the rules and procedures for all individuals accessing and using the institution's IT assets and resources. It outlines rules and guidelines for user and IT personnel behavior while also identifying consequences for not adhering to them.

Al- Ameen College give due consideration to the availability, protection and confidentiality of information technology resources of the institution. For this purpose it has implemented an IT policy document which applies to all faculty, staff and students of Al – Ameen College. The institution presumes all staff and students to abide to the policies. The institution provides updated IT resources to support educational, institutional, research and administrative activities of staff and students.

College expects that the stake holders should be fully aware of their responsibilities while using this privilege. This policy statement gives guidance to the staff and students on the procedures and principles related to utilization of ICT resources of college and also provides general awareness to them on their obligations and responsibilities while using the same.

Stake holders should be fully aware of the fact that these resources are provided by the college only as a privilege and it is not their right. Therefore, the use of these resources should be limited to carrying out their duties in conducting the business of Al-Ameen College and for academic purposes. They should refrain from its use for other purposes unless they get necessary permission from the authorized persons.

Proper and efficient use of ICT tools and internet facilities will allow the teachers and students to access unlimited opportunities and knowledge apart from opening contact and to communicate with organizations, groups and individuals worldwide which in turn will help them to boost their competence, expertise and knowledge. Apart from this, ICT tools will help the students to become more self-motivated and will make them digitally fit as to face the challenges posed by ever changing technology.

IT Resources include:

- 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, Surveillance network
- Learning Management Systems
- Other governing software, etc.

Need for IT Policy

To maintain security and ensure legal and appropriate use of IT infrastructure in the campus, institution formulated an IT Policy. This policy provides guidelines on the Dos and Do not's of using IT resources of the institution. The policy primarily focus on the protection and safeguarding of confidentiality, integrity and availability of information assets that are created, accessed, managed, or controlled by the institution. Information assets addressed by the policy include data, information systems, computers, network devices, as well as documents and verbally communicated information. In addition, this policy supports effective organizational security and protects users and IT resources from, but not limited to cyber criminals, bullying, misuse of accounts and assets as well as the spread of malicious software

IT Policy provides a safe and secure environment where the IT resources can be handled by students, faculty, staff and Management in a transparent, reliable and efficient way. The users of the IT resources must ensure that they use these resources for teaching, learning, research, innovations, and administration.

The following are the major focal points for establishing IT policy in the institution:

- To facilitate access of IT resources to all students and staff in the institution.
- To upgrade the IT resources from time to time
- Introduce new IT technologies in the College
- Annual Maintenance Services of IT resources
- Provide safe and secure IT operations in the institution
- Installation of firewalls, virus checking and content filtering

The lack of IT policies will throw challenges in managing IT resources and networking in the institutions. Users of the IT resources will feel totally free while accessing the resources and this absence of policies and guidelines will lead to unsecure and unjustified use of resources. Al – Ameen College, thus maintains and operates a well-defined IT policy to safeguard its IT resources.

Roles and Responsibilities

The institution envision the following roles and responsibilities from each users:

1) The IT Department shall undertake all appropriate controls to ensure that all users are complying with the policy.
2) The users of the IT resources should ensure that the usage is limited to academic, research. Innovation etc
3) All users have to comply to the existing national, state and other applicable laws
4) Stake holders must ensure that all the data pertaining to the college is fully secured and protected through passwords. (Passwords should be complex with numbers, special characters, upper case letters and lower case letters)
5) All the users are expected to respect copyrights, licenses, contractual agreements and intellectual property rights. They should use only the accounts and facilities that they are authorized to use and should not trespass without due permission
6) No user is allowed to operate equipment's and facilities of the college that they are not authorized to use
7) Users are not allowed to share their account details with anybody else
8) Users should not interrupt the work of other faculty or students while using IT resources of the college
9) Users are not supposed to access pornographic sites or publish obscene, derogatory or defaming materials that threatens and infringes basic human rights by using college ICT facilities
10) Users should not delete, disclose or copy the materials and data stored in the resources of the college without explicit permission from the authorized

person/ persons

11) Users cannot make any public display of college information in social networking sites without getting due permission. All kinds of political propaganda is banned.

12) Users are not supposed to indulge themselves in acts like spreading viruses, phishing, chain letters, pyramid solicitations etc. which will be violation of the principles of the college.

N.B: *Any violation of the above code of conduct will lead to disciplinary proceedings.

*College reserves the right to access and use of its IT resources and will have the authority towithdraw its use without assigning any reason therefore.

IT Hardware Installation Policy.

The user community of the institution has to note several precautions while installing their computers or peripherals so as to safeguard the disruption of services in future while they are handling these devices.

a) **Primary User**: An individual in whose room the computer is installed and is primarily used by him/her is considered to be “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

b) **End User of Computer Systems**: Apart from the client PCs used by the users, the institute will consider servers not directly administered by Network unit, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the Network unit, are still considered under this policy as "end- users" computers.

c) **Warranty & Annual Maintenance Contract:** Computers purchased by any Department/Cells should preferably be with 3-year on- site comprehensive warranty. After the expiry of warranty, computers would be maintained by Network unit through the help of system administrators or by external Service Engineers on call basis. Such maintenance should include OS re-installation and checking virus related problems also.

d) **Power Connection to Computers and Peripherals**: All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

e) **Network Cable Connection:** While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as

they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

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

g) **Maintenance of Computer Systems provided by the Institute**: For all the computers that were purchased by the institute centrally and distributed by the IT Cell and will attend the complaints related to any maintenance related problems. The maintenance and utilisation of IT facilities will be handled effectively by IT cell and System Administrators. An annual maintenance is scheduled periodically which includes servicing, installation of software's, antivirus and up gradation. The system administrators will address the issues reported to them through complaint registers,

intercom, mobile or personally immediately and follow up the procedures. If still problem persists, help from external expertise or external servicing is sought. A log book of the computer lab is also maintained to monitor the utilisation of IT facilities.

h) **Noncompliance:** The network user community of the institution including students, staff and faculty 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 data and records and 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.

i) **IT Cell Interface:** IT Cell 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/phone. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The IT Cell and system administrators will provide guidance as needed for the individual to gain compliance.

Software Installation and Licensing Policy

Any computer purchases made by the individual departments/cells should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed. Respecting the anti-piracy laws of the country, Institute IT policy does not allow any pirated/unauthorized software installation on the institute owned computers and the computers connected to the institute campus network. In case of any such instances, institute will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

a) **Operating System and its Updating**: Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their

computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Al – Ameen College has made it 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.

b) **Antivirus Software and its updating:** Computer systems used in the College should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy. 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 IT Cell.

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 many volumes typically C, D and so on. OS and other software should be on C drive and user's data files on the other drives (e.g. D, E). 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 on CD / DVD or other storage devices such as pen drives, external hard drives.

c) **Noncompliance**: The faculty, staff, and students of Al – Ameen College 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 institute. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

d) **IT Cell / Computer Center Interface:** IT Cell or system administrators upon finding a non-compliant computer will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/phone. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The IT Cell will provide guidance as needed for the individual to gain compliance.

Web Site Hosting Policy

a) **Official Pages**: Departments, Clubs, Cells, may have pages on the official Web Site of Al – Ameen College. IT Cell and the web site coordinator is responsible for maintaining the official web site of the institute viz., https://www.alameencollege.org/

b) **Personal Pages:** It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal pages linked to official web site of the institute by sending a written request or mail to IT Cell / Website coordinator giving the details of the hyperlink of the URL that he/she wants to be added in the official web site of the institute. However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws. Personal pages also will not include the hosting of pages for other individuals or groups. Personal pages should explicitly mention that views expressed by him/her in their pages are exclusively their own and not that of the institute.

b) **Responsibilities for updating Web Pages**: Departments, cell, and individuals are responsible to send updated information time to time about their Web pages to IT Cell and Website Coordinator.

o

Network (Intranet & Internet) Use Policy

Network connectivity provided either through an authenticated network access connection or a Virtual Private Network (VPN) connection, or Wi-Fi is governed under the Institute IT Policy. The IT Cell is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the Institute's network should be reported to IT Cell.

a) **IP Address Allocation:**

Any computer (PC/Server) that will be connected to the institute network should have an IP address assigned by the IT Cell. Departments should follow a systematic approach, the range of IP addresses that will be allocated to each group as decided. So, any computer connected to the network from that group 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 unauthorized from any other location. As and when a new computer is installed in any location, the concerned user has to take IP address allocation from IT Cell / respective department. An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports.

b) **DHCP and Proxy Configuration by Individual Departments /Cells/ Users**:

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the institute. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by Computer Center. 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 Network connectivity provided through an authenticated network access connection or Wi-Fi is governed under the Institute IT Policy. The

IT Cell is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the Institute's network should be reported to the IT Cell or System Administrators.

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 IT Cell/ System Administrator 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. IT Cell takes no responsibility for the content of machines connected to the Network, regardless of whether those machines belong to the college or individuals. IT Cell 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 IT Cell. 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:**

1. 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 IT Cell including Point of Contact information.

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

3. 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.

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

Email Account Usage Policy

In an effort to increase the efficient distribution of critical information to all faculties, staff and students, and administrators, it is recommended to utilize the institute's e-mail services, for formal communication and for academic & 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 Institute to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general Institute messages, official announcements, etc. To receive these notices, it is essential that the e-mail address be kept active by using it regularly. For obtaining the institute's email account, user may contact IT Cell for email account and default password by submitting an application in a prescribed proforma.

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

- 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 institute's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

- 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.

- 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

- 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.

- 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 college IT security policy.

- It is ultimately each individual's responsibility to keep their e-mail account free from violations of college's email usage policy.

- 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@shcollege.ac.in for necessary action to delete from the spam mail category. It is recommended to empty this folder as frequently as possible.

Video Surveillance Policy CCTV

The system comprises:

Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs. Cameras will be located at strategic points on the campus, principally at the entrance and exit point of buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation. 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 Camera installation is in use. 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.

Purpose of the system:

The system has been installed by institute with the primary purpose of reducing the threat of crime generally, protecting college premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy.

These purposes will be achieved by monitoring the system to:

• Deter those having criminal intent

• Assist in the prevention and detection of crime

• Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order

• Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

The system will not be used:

• To provide recorded images for the world-wide-web.

- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

It is recognized that members of institute and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the IT Cell. CCTV footage provided by the College (IT Cell) upon receiving the requests from the individuals on prescribed proforma.

Access to images

- All access to images will be recorded in the Access Log as specified in the Procedures Manual
- Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.
- Access to images by third parties : Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:
  - Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder.
  - Prosecution agencies
  - Relevant legal representatives
  - The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
  - People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
  - Emergency services in connection with the investigation of an accident.

College Database Policy

This Policy relates to the databases maintained by the College. Data is a vital and important resource for providing useful information. Its use must be protected even when the data may not be confidential. Al – Ameen College has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the institute's approach to both the access and use of this College resource.

1. **Database Ownership**:

Al – Ameen College is the data owner of the entire institutional data generated in the campus.

2. **Data Administrators**:

Data administration activities outlined may be delegated to some of the officers in that department.

3. **MIS Components**:

For the purpose of Management Information System requirements of the institute these are: -

Employee Information Management System.

Students Information Management System.

Financial Information Management System.

Library Management System.

Document Management & Information Retrieval System.

Learning Management System

Here are some general policy guidelines and parameters for departments, cells and administrative department data users:

1. The data policies of College do not allow the distribution of data that is identifiable to a person outside the institute.

2. Data from the College's Database including data collected by departments or individual faculty and staff, is for internal institute purposes only.

3. One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies

the institute makes information and data available based on those responsibilities/rights.

4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office.

5. Requests for information from any courts, attorneys, etc. are handled by the Office and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office for response.

6. All Departments, Clubs and cells provide information and reports to IQAC periodically and IQAC compiles and stores data for submission of various reports to Management, MHRD, AISHE, NAAC, NIRF and other agencies.

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

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

Responsibilities of IT Cell

a) **Campus Network Backbone Operations**

IT cell act as the campus network backbone and administers, maintains and controls its active components in the campus. IT cell operates the campus network backbone such that service levels are maintained as required by the Departments, Clubs, Cells and hostels served by the campus network backbone within the constraints of operational best practices.

b) **Maintenance of Computer Hardware & Peripherals**

IT cell is responsible for maintenance of the institute owned computer systems and peripherals that are under warranty or out of the warranty.

c) **Receiving Complaints**

IT Cell / System Administrator may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them is having any problems. The designated person in IT Cell receives complaints from the users of these computer systems and coordinates with the service engineers of the respective brands of the computer systems (which are in warranty) to resolve the problem within a reasonable time limit. For out of warranty computer systems, problems resolved at computer center. Computer Center may receive complaints from department/users, if any of the networks related problems are noticed by them such complaints should be made by email/phone. IT Cell may receive complaints from the users if any of the user is not able to access network due to a network related problem at the user end. Such complaints may be generally through phone call. The designated person in IT Cell receives complaints from the users and coordinates with the user/service engineers of the network hardware or with internal technical team to resolve the problem within a reasonable time limit.

e) Scope of Service

IT Cell will be responsible for solving the hardware related problems or OS or any other application software that were legally purchased by the institute and was loaded by the company as well as network related problems or services related to the network.

f) Installation of Un-authorized Software

IT cell 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.

f) Physical Demarcation of Campus Buildings' Network

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

g) Network Expansion

Major network expansion is also the responsibility of IT Cell. Every 3 to 5 years, IT Cell reviews the existing networking facilities, and need for possible expansion.

h) Wireless Local Area Networks

1. Where access through Fiber Optic/UTP cables is not feasible, in such locations IT Cell considers providing network connection through wireless connectivity.
2. IT Cell is authorized to consider the applications of Departments, or divisions for the use of radio spectrum from IT Cell prior to implementation of wireless local area networks.
3. IT Cell is authorized to restrict network access to the Cells, departments, or hostels through wireless local area networks either via authentication or MAC/IP address restriction

i) Electronic logs

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

j) Global Naming & IP Addressing

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

k) Providing Net Access IDs and email Accounts

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

l) Disconnect Authorization

IT Cell will be constrained to disconnect any Department, or cell, club, hostel 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 Department, or cell, hostel machine or network, IT Cell endeavors to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Department or cell is disconnected, IT Cell provides the conditions that must be met to be reconnected.

Responsibilities of Department

a) User Account

Any Centre, department, or cell or other entity can connect to the College network using a legitimate user account (Net Access / Captive Portal ID) for the purposes of verification of affiliation with the College. The user account will be provided by IT Cell, upon filling up the prescribed application form and submitting it to IT Cell / System Administrator.

Once a user account is allocated for accessing the institution's computer systems, network, mail and web services and other technological facilities, that account holder is personally responsible and accountable to the institute for all the actions performed using that user account. Hence, users are advised to take reasonable measures such as using complex passwords, not sharing the passwords with others, not writing down the password at a place which is accessible to others, changing the passwords frequently and keeping separate passwords for Net Access Id and for email account ID to prevent un-authorized use of their user account by others. It is the duty of the user to know the IT policy of the institute and follow the guidelines to make proper use of the institute's technology and information resources.

b) Supply of Information by Department, or Cell for Publishing on /updating the Web Site of Al – Ameen College

All Departments or Cells should provide updated information concerning them periodically (at least once in a month or earlier). Hardcopy or softcopy to be sent to the IT Cell. This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by Department, or Cells. Links to any web pages that have to be created for any specific purpose or event for any individual department or faculty can be provided by the IT Cell upon receiving the written requests. If such web pages have to be directly added into the official web site of the College, necessary content pages (and images, if any) have to be provided by the respective department or individual in a format that is exactly compatible with the existing web design/format. Further, such requests along with the soft copy of the contents should be forwarded to the System Administrator, IT Cell well in advance.

c) Security

In connecting to the network backbone, department agrees to abide by this Network Usage Policy under the institutions 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

d) 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 College are the property of the College and are maintained by Computer Center and respective departments. Tampering of these items by the department or individual user comes under violation of IT policy.

e) Additions to the Existing Network

Any addition to the existing network done by department or individual user should strictly adhere to the college network policy and with prior permission from the competent authority and information to IT Cell. College Network policy requires following procedures to be followed for any network expansions:

1. UTP cabling should follow structured cabling standards. No loose and dangling UTP cables are drawn to connect to the network.

2. UTP cables should be properly terminated at both ends following the structured cabling standards.

3. Only managed switches should be used. Such management module should be web enabled. Managed switches give the facility of managing them through web so that IT Cell can monitor the health of these switches from their location. However, the hardware maintenance of so expended network segment will be solely the responsibility of the department/individual member. In case of any network problem created by any computer in such network, if the offending computer system is not locatable due to the fact that it is behind an unmanaged hub/switch, the network connection to that hub/switch will be disconnected, till compliance is met by the user/department.

4. As managed switches require IP address allocation, the same can be obtained from IT Cell on request.

f) **Campus Network Services Use Agreement**

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

g) **Enforcement**

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

Responsibilities of the Administrative Department

IT Cell needs latest information from the different Administrative Department for providing network and other IT facilities to the new members of the institute and for withdrawal of these facilities from those who are leaving the institute, and also for keeping the Al – Ameen College 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.
- Information about Termination of Services.
- Information of New Enrolments.
- Information on Expiry of Studentship/Removal of Names from the Rolls.
- Information on Important Events/ Achievements.
- Information on different Rules, Procedures, and Facilities.

Guidelines for Desktop Users

These guidelines are meant for all members of the Al – Ameen College Network User. Due to the increase in hacker activity on campus, College IT Policy has put together recommendations to strengthen desktop security.

The following recommendations include:

1) All desktop computers should have the latest version of antivirus. And should retain the setting that schedules regular updates of virus definitions from the central server.

2) When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be a balance between loss

of productivity (while patches are applied) and the need for security. Whenever possible, security policies should be set at the server level and applied to the desktop machines.

3) The password should be difficult to break.

4) The guest account should be disabled.

5) In addition to the above suggestions, IT Cell recommends a regular backup strategy. It should be noted that even with all the procedures listed above; there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine

Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT Cell. On receipt of notice (or where the College otherwise becomes aware) of any suspected breach of this Policy, Al – Ameen College reserves the right to suspend a user's access to College Data. If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the institutions disciplinary procedures.

Revisions to the Policy

Al – Ameen College reserves the right to revise the terms of this Policy at any time. Any such revisions will be noted in the revision history of the policy, which are available on the website of the College and by continuing to use the IT Resources of the College following any update it is considered acceptance on the revised terms of this Policy.

APPENDIX I

AL - AMEEN COLLEGE

EDATHALA, ALUVA – 683561

Campus Wi-Fi / Network Services Use Agreement

Read the following important policies before applying for the user account/email account. By signing the application form for IP address allocation/Net Access ID (user account) /email account, you agree to act in accordance with the IT policies and guidelines of Al – Ameen College. Failure to comply with these policies may result in the termination of your account/IP address. It is only a summary of the important IT policies of the college. The user can have a copy of the detailed document from the Intranet. (https://www.alameencollege.org/iqac/quality-policy/) A Net Access ID is the combination of a username and a password whereby you gain access to college computer systems, services, campus networks, and the internet.

I. Accounts and Passwords

The User of a Net Access guarantees that the Net Access ID will not be shared with anyone else. In addition, the Net Access ID will only be used primarily for educational/official purposes. The User guarantees that the Net Access ID will always have a password. The User will not share the password or Net Access ID with anyone. Network ID's will only be established for students, staff and faculty who are currently affiliated with the College. Students, staff and faculty who leave the College will have their Net Access ID and associated files deleted. No User will be allowed more than one Net Access ID at a time, with the exception that faculty or officers, who hold more than one portfolio, are entitled to have Net Access ID related to the functions of that portfolio.

II. Limitations on the use of resources

On behalf of the College, IT Cell reserves the right to close the Net Access ID of any user who is deemed to be using inordinately large amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

III. Computer Ethics and Etiquette

The user will not attempt to override or break the security of the College computers, networks, or machines/networks accessible there from. Services

associated with the Net Access ID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of threatening, harassing, abusive, obscene or fraudulent messages. Even sending unsolicited bulk e-mail messages comes under IT Policy violation. In addition, the User agrees to adhere to the guidelines for the use of the particular computer platform that will be used. User's Net Access ID gives him/her access to email, and campus computing resources. The use of these resources must comply with College policy and applicable.

Electronically available information

(1) May not contain copyrighted material or software unless the permission of the copyright owner has been obtained,

(2) May not violate College policy prohibiting sexual harassment,

(3) May not be used for commercial purposes,

(4) Should not appear to represent the College without appropriate permission, or to represent others,

(5) May not appear to represent other organizations or companies,

(6) May not contain material which violates pornography laws, or algorithms or software which if transferred violate laws,

(7) May not contain scripts or code that could cause a security breach or permit use of resources in opposition to College policy, and

(8) WWW pages should clearly show identifying information of the owner of the page and we suggest that it also shows date of last revision and an address (e-mail or postal) for correspondence.

IV. Data Backup, Security, and Disclaimer

IT Cell or System Administrator 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 Cell or System Administrator staff member in the process of helping the user in resolving their network/computer related problems. Although IT Cell / System Administrator 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.

In addition, IT Cell 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 IT Cell or System Administrator, as part of Al- Ameen College, harmless for any such liability or expenses. AL- AMEEN COLLEGE retains the right to change and update these policies as required without notification to the User.

IV. Account Termination and Appeal Process

Accounts on AL - AMEEN COLLEGE network systems may be terminated or disabled with a short/without notice for any of the reasons stated above or for other inappropriate use of computing and network resources. When an account is terminated or disabled, IT Cell will make an attempt to contact the user (at the phone number they have on file with IT Cell / System Administrator) and notify them of the action and the reason for the action. If the termination of account is of temporary nature, due to inadvertent reasons and are on the grounds of virus infection, account will be restored as soon as the user approaches and takes necessary steps to get the problem rectified and communicates to the IT Cell of the same.

But, if the termination of account is on the grounds of wilful breach of IT policies of the college by the user, termination of account may be permanent. If the user feels such termination is unwarranted, or that there are mitigating reasons for the user's actions, he or she may first approach the coordinator of IT Cell / System Administrator, justifying why this action is not warranted. If the issue is not sorted out he/she may appeal to the Appeals Board duly constituted by the college for this purpose to review the evidence and hear reasons why an appeal should be considered.

If the Appeals Board recommends revival of the account, it will be enabled. However, the IT Cell of the Appeals Board is final and should not be contested. Users may note that the College's Network Security System maintains a history of infractions, if any, for each user account. In case of any termination of User Account, this history of violations will be considered in determining what action to pursue. If warranted, serious violations of this policy will be brought before the appropriate College authorities.

APPENDIX II

AL - AMEEN COLLEGE

EDATHALA, ALUVA - 683561

REQUEST FORM FOR OFFICAL E-MAIL ACCOUNT

Faculty/Administrative Staff/ Student

1. Full Name :

2. Designation/ Register Number :

3. Department :

4. Mobile Phone :

5. Personal E-mail ID :

6. Existing E-mail ID :

Date: **Signature of the Applicant**

- **For Office Use**

The following email ID is created for Prof./Dr./Mr./ Ms

.....

.....

.....on.....

@alameencollege.org

Signature on Behalf of Co-ordinator, IT CELL

APPENDIX III

AL - AMEEN COLLEGE

EDATHALA, ALUVA - 683561

REQUEST FORM FOR NET ACCESS

Faculty/Administrative Staff/ Student

1. Full Name :

2. Designation :

3. Department :

4. Mobile Phone :

5. E-mail ID :

Date: **Signature of Applicant:**

....

For Office Use

Net access ID is activated for the applicant.

Signature on Behalf of Co-ordinator, IT CELL

APPENDIX IV

AL - AMEEN COLLEGE

EDATHALA, ALUVA - 683561

REQUEST FORM FOR CCTV FOOTAGE

Faculty/Administrative Staff/ Student

1. Full Name :

2. Designation / Register No :

3. Department :

4. Mobile Phone :

5. E-mail ID :

6. Date of Footage :

7. Time : From ..... To .....

8. Camera Location :

9. Description: .....

Date: **Signature of Applicant:**

....

For Office Use

CCTV Footage is given to the applicant

Signature on Behalf of Co-ordinator, IT CELL