ISLAMIAH COLLEGE (Autonomous), VANIYAMBADI

IT Policies & Guidelines

Prepared by
IT Committee
Islamiah College
Vaniyambadi 635752

TABLE OF CONTENTS

Islamiah College Information Technology Policy

Need for IT Policy

An institutions IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the institution on the campus.

This policy establishes institution wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University.

Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information

Islamiah College IT policy

Islamiah College Information Technology (IC-IT) provides a wide range of computing resources to bridge the educational mission and administration of the College. Information Technology Service provides and maintains the campus backbone network, administrative servers, e-mail and web servers, public computing facilities, and institutional electronic gadgets and computer systems.

- ITS have become an important resource for academic, administrative and research processes for members of the College users.
- The College user are encouraged to use these resources, provided they respect the rights of others, abide by the rules and regulations of the College, and hold the responsibility for safeguarding the College's computing environment.
- Use of ITS resources is considered an agreement to abide by this policy. Users found in violation may be subject to penalties of varying degrees, including temporary or permanent denial of access to ITS resources and services. Violators may also be subject to action by campus, civil, or criminal judicial systems.

Preamble:

Internet & intranet are major resources of information in an educational institution. Islamiah College is committed to promote and develop student learning and reasoning by providing suitable right IT infrastructure. The IT policies are designed to recognize the problems related to uncontrolled surfing by the users:

- Prolonged or intermittent surfing, affecting quality of work
- Heavy downloads that lead to choking of available bandwidth
- Exposure to legal liability through embarrassing content.
- Confidential information being made public.

Standardized IT resources:

IC-IT has to establish a standard set of equipment for Development of Information and Communication System.

The items designated as standard by IC-IT are :

a) Desktops
b) Laptops
c) Tablets
d) Printers - Small (Desktop)
e) Printers - Medium (Workgroup)
f) Printers - Large (Department)
g) Multifunction Printer/Copy/Scan/Fax Devices
h) Black and White Copiers
i) Color Copiers
j) Servers (Computing or Application)
k) Storage Units (Disk/Tape Units and Network
l) Smart Phones (Android or iOS)
m) All Networking and Telecommunications Equipment
n) Audio/Visual Equipment/CCTV Infrastructure
o) Software

NETWORK ACCESS POLICY APPLICABLE FOR THE USER

- User shall take prior approval from the competent authority to connect the client system to the network
- A client system authorized to connect to one network shall not connect to any other network
- For wireless connectivity, user shall ensure the following:
  1. By default, the wireless interface is at the time of examination.
  2. Client system may not connect to wireless net from the computer authority.
  3. If permitted, the wireless interface of the client system may be enabled to connect with authorized wireless network only.

  Client System Log

  User having administrative privileges shall not disable/delete the audit trials/logs on client system

ACCOUNT PROVISIONING AND ACCESS CONTROL STANDARDS

Accounts that access electronic computing and information resources require prudent oversight. The following security precautions should be part of account management:

- All accounts must have a password that adheres to the practices outlined in the Password Management Policy document.
- Any account that is not used for interactive login or authentication must be “locked” or “disabled” according to the definition of those terms for the particular OS in question.
- Prior to creating a user account, that user’s affiliation with the college must be verified by the sponsoring unit or division (i.e., Human Resources, Dean).
- Users must attend all appropriate application or data handling training courses prior to their account being activated.

- There may be only one user associated with an account. Users may NOT share an account.
- Accounts should not be granted any more privileges than those that are necessary for the functions the user will be performing.
- Directory and file permissions should be set correctly to prevent users from listing directory contents or reading, modifying, or deleting files that they are not authorized to access.
- Account setup and modification shall require the signature of the account requestor, the requestor's immediate supervisor, the data owner and the Office of Information Technology.
- The organization responsible for a resource shall issue a unique account to each individual authorized to access that networked computing and information resource. It is also responsible for the prompt deactivation of accounts when necessary, i.e., accounts for terminated individuals shall be removed/disabled/ revoked from any computing system at the end of the individual's employment.
- The identity of users must be authenticated before providing them with account and password details. If an automated process is used, then the account holder should be asked to provide several information items that in totality could only be known by the account holder.
- Passwords for new accounts should NOT be emailed to remote users unless the email is encrypted.
- The date when the account was issued and its expected expiration date (if applicable) should be recorded in the dashboard.

SECURITY

System Admin maintains the Servers offline, Synchronization the data to intranet to internet when it is required, he is in charge for the security of information stored on those systems and for keeping those systems free from unauthorized access.

INTERNET

The Internet is an unsupervised environment and staff members and students must exercise appropriate guidance and discernment with WIFI services. It is the responsibility of users to ensure that their behavior does not breach College policies, rules or requirements, or state or federal legislation. Individuals accessing the Internet, despite the presence of filtering software that may limit access to certain sites, may encounter inappropriate material or be in contact with undesirable individuals when communicating. The College is acutely aware of the potential difficulties however it believes that the benefits far outweigh the potential problems.

SOCIAL NETWORKING

Students may interact with staff members for educational purposes using on-premise social networking technologies such as the Islamiah College Learning Management System (ICLMS). However, in the event that College-sanctioned student teacher interactions on external social networking sites are required, parent and guardian permission will be sought prior to the interaction taking place.

WEBSITE POLICY

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the institution website.

Procedures for Website Register

The website register must record the following details:

• List of domain names registered to the institution

• Dates of renewal for domain names

• List of hosting service providers

• Expiry dates of hosting .

WEBSITE CONTENT

All content on the institution website is to be accurate, appropriate and current. This will be the responsibility of System Administrator. All content on the website must follow institution approval .

EMERGENCY MANAGEMENT OF INFORMATION TECHNOLOGY

Purpose of the Policy This policy provides guidelines for emergency management of all information technology within the institution.

Procedures IT Hardware Failure Where there is failure of any of the institution's hardware, this must be referred to System Administrator immediately.

It is the responsibility of System Administrator to take remedial measures in the event of IT hardware failure.

It is the responsibility of System Administrator to undertake tests on planned emergency procedures quarterly to ensure that all planned emergency procedures are appropriate and minimize disruption to institution operations.

VIRUS OR OTHER SECURITY BREACH

IC-Information technology is compromised by software virus or hacking, such breaches are to be reported to System Administrator immediately. System Administrator is responsible for ensuring that any security breach is dealt with within a week to minimize disruption to institution operations.

Antivirus Software and its updating

1. 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.

2. Individual users should make sure that respective computer systems have current virus protection software installed and maintained. He should make sure that the software is running correctly.

STORAGE

All files and other data will be stored on the file server. The fileserver is backup every weekend and labeled in external Hard drive. At least 3 years of information are recorded.
Backups of Data: Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into two volumes typically C and D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted.

IT Hardware Installation Policy

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

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

B. Warranty & Annual Maintenance Contract
   Computers purchased by any Section/Department/Project should preferably be with 3-year onsite comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include OS re-installation and checking virus related problems also.

C. 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. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

D. 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.

E. 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.

F. Shifting Computer from One Location to another
Computer system may be moved from one location to another with prior written intimation to the Principal as a record of computer identification names and corresponding IP address is maintained.

Software Installation and Licensing Policy

Any computer purchases made by the individual departments should make sure that such computer systems have all licensed software (operating system, antivirus software an necessary application software) installed. Respecting the anti-piracy laws of the country, college IT policy does not allow any pirated/unauthorized software installation on the college owned computers and the computers connected to the college network.

E-waste management policy:

The colleges try to recycle the electronic items to its best. E-waste are disposed through Government authorized e-waste management vendor.

PRINCIPAL
(Dr. T. MOHAMED ILYAS)