YENEPOYA
INSTITUTE OF TECHNOLOGY

Affiliated to VTU, Belgavi and Approved by AICTE, Delhi

INFORMATION TECHNOLOGY DEPARTMENT

POLICY GUIDELINES

Table of contents

1. Introduction to the policy

Information Technology has been globally recognised as an essential vehicle of "growth and development" in the new millennium. Yenepoya Institute of Technlogy has taken up Information Technology & Communication (IT) as the principal engine of rapid growth. The IT departments committed to deploying IT services as an effective tool for catalysing accelerated and efficient governance in Institute operation

Statement of purpose:

The purpose of this IT policy is to outline the acceptable use guidelines for IT equipment and services at the Institution. This policy intends to promote a culture of openness, trust, and integrity. These are general guidelines on what can be done, and what should not be done, on the Institution IT infrastructure to ensure efficient and effective use of Institution IT resources; protect IT resources from injurious actions, including virus attacks, data loss, unauthorised access, network, and system failures, and legal problems.

This policy seeks to guide designers, developers, and users of Information and IT resources on appropriate standards to be adopted at the Institution. Its objectives include to:

- Guide in developing a pervasive, reliable and secure communications infrastructure conforming to recognised International standards supporting all services in line with the priorities of the Institution;
- Provide a framework for the development and management of IT network services that shall ensure the availability, reliability, enhanced performance, security, and reduce the cost of running the IT infrastructure;
- Establish information requirements and implement security across the Institution's IT infrastructure;
- Provide a framework, including guidelines, principles, and procedures for the development and implementation of management information systems in the Institution;
- Guide the handling of organisational information within the IT department and the Institution as a whole by ensuring compliance with applicable statutes, regulations, and mandates for the management of information resources; and thereby establish prudent practices on the internet and the Institution intranet use;
- Uphold the integrity and image of the Institution through defined standards and guidelines for ensuring that the content of the Institution's websites is accurate, consistent and up-to-date;
- Serve as the direction pointer for the IT's mandate in supporting users, empowering them towards making maximum use of IT services and resources and specifying the necessary approaches;
- To guide the process of enhancing user utilisation of IT resources through training;
- Outline the rules and guidelines that ensure users' PCs, and other hardware are in serviceable order, specifying best practices and approaches for preventing failure;

2. Network development and management policy

Introduction

The information and communications infrastructure at the Institution have evolved into a vast, complex network over which the education, research, and business of the Institution is conducted. It is envisaged that the network will integrate voice, data, and video, to form a unified information technology resource for the Institution community. Such a network shall demand adherence to a centralised, coordinated strategy for planning, implementation, operation, and support. Decentralisation shall be implemented through appropriate Institution structures.

The Institution network functions shall be broken down into the following areas:

Campus Local Area Networks (LANs)

Wireless networks

Connection to, access and usage of IT facilities

New or changed use of IT equipment

Monitoring of network performance.

This, therefore, shall require a policy that will secure the future reliability, maintainability, and viability of this valuable asset.

Objectives

The objective of this policy is to establish a comprehensive and uniform Network Development & Management policy for the administration of the Institution IT infrastructure.

This policy defines the arrangements and responsibilities for the development, installation, maintenance, and use and monitoring of the Institution 's networks to ensure that, these networks are adequate, reliable, and resilient to support continued high levels of activity.

This policy applies to any person accessing or using the IT infrastructure owned, managed, supported, or operated by, or on behalf of the Institution. These include all Institution staff and students; any organisation accessing services over Institution IT networks; persons contracted to repair or maintain the Institution's IT networks; and suppliers of network services.

The Institution will develop and support an Institution -wide IT network as an underlying infrastructure service for the facilitation of sharing electronic information and resources by all members of the Institution. This includes all staff and students of the Institution, and other persons engaged in legitimate Institution business as may be determined from time to time.

The Institution network will be designed and implemented in such a way as to serve those located at the Institution campuses and, to a lesser extent, those located elsewhere.

The ultimate goal is that every room in the Institution in which research, teaching, learning, or administration functions take place should be connected. And every member of the Institution should have the capability to access the Institution IT infrastructure.

The network will form part of the general fabric or infrastructure of the Institution.

There will be one coherent network supporting access to all general information services provided to the Institution members.

High levels of availability, reliability, and maintenance will be major objectives in the construction and operation of the Institution IT network.

The design and construction of the Institution network will take into account emerging technologies and standards wherever possible.

Before the installation of the "live" situation, major network developments shall be "soak-tested" an off-line simulation.

For up to two months after the live installation of the new development, the network provider that it is to be replaced shall, wherever possible, remain in place as a "fall-back" in the event of any subsequent failure of the new development when it is subject to actual user demand.

IT network provision in new and refurbished buildings

Network provision for new and refurbished buildings shall be made following the specification published from time-to-time by the IT Department.

Where the network requirements are of specialised nature, the Head of the Facility/Department concerned shall seek further guidance from the IT Department.

All new buildings to be erected in the Institution shall incorporate an appropriate structured cabling system to allow connection to the Institution network.

The Institution network will consist of several parts: "Backbone" systems, a collection of inter-building connections; "Campus LANs," wireless networks (Hotspots)

The Institution network backbone will comprise an inter-building cabling system, together with one or more "Gateway" interfaces at each building or in the path to each building which will connect the backbone to the network(s) within each building.

Structure of Institution backbone

The Institution network backbone shall connect, singly or severally, to buildings, not to individual departments or units.

The planning, installation, maintenance, and support of the Institution network backbone shall be under the control of the IT department.

Connection to the Institution network backbone shall be approved by the IT department.

The Institution network backbone at any particular point of time will be aimed at facilitating the traffic flow between connected buildings or networks.

Structure of campus LANs

Wherever feasible, the network(s) within each building shall be arranged so that there is a point of connection to the Institution network backbone. In cases where it is not possible to establish a single connection, multiple building gateways may be installed.

Network protocols used on building networks and communicating through the gateway must use approved configuration parameters, including approved network identifiers.

Building networks connecting to the Institution network shall meet overall Institution network security and management requirements.

Wireless networks

Wireless LAN also is known as hotspot or Wi-Fi are networks rolled out using radio waves to provide mobile network access as defined under IEEE 802.11 protocol.

Structure of wireless networks.

Installation, configuration, maintenance, and operation of wireless networks serving on any property owned by the Institution, are the sole responsibility of the IT department. Any independently installed wireless communications equipment is prohibited.

Wireless access points shall terminate at a point of connection to the Institution network backbone. In cases where it is not feasible to establish a single connection, multiple wireless gateways may be installed limited to a maximum of three hops.

Wireless networks connecting to the Institution network shall meet overall Institution network security and management requirements, including approved network identifiers.

Access to IT facilities

Server Rooms, network racks, and IT network equipment

All server rooms and network racks shall be locked at all times.

Entry to server rooms and network racks, and interference with IT network equipment is strictly prohibited.

Other than in an emergency, access to server rooms and network racks and IT network equipment shall be restricted to designated members of staff of the IT department. Any necessary access must have the prior written consent of the IT Department.

Access in an emergency

In the event of a fire or other emergency, security staff and/or staff of the maintenance department and/or the emergency services may enter these areas, without permission, to deal with the incident.

Network equipment

Only designated members of the staff of IT are authorised to install and maintain active network equipment, including hubs, switches, and routers connected to the Institution's IT networks.

Connection to and usage of IT facilities

All connections to the Institution's IT networks must conform to the protocols defined by the IT Department and with the requirements that apply to Internet Protocol (IP) addresses.

Only designated members of staff of the IT department, or other staff explicitly authorised by the IT , may make connections of desktop services equipment to the IT network.

External access to servers on the backbone network
External access means access by a person's external to the Institution; access to the backbone network from external locations.
Where specific external access is required to servers on the backbone network, the IT Department shall ensure that this access is strictly controlled and limited to specific external locations or persons.
The IT Department will monitor compliance with access arrangements as stipulated in this IT Policy and the relevant IT security policy on server security issued by the Institution from time to time.
Suspension and/or termination of access to IT networks

A user's access to the Institution's IT networks will be revoked automatically

At the end of studies, employment or research contract.

At the request of the Principal of Faculty/Head of Resource Centre/Head of Department or Head of Unit.

Where there is a breach of these regulations

The Institution reserves the right to revoke a user's access to the Institution's IT network where the user is suspended under a disciplinary investigation.

The Principal will establish mechanisms to ensure that changes in student/employment status are communicated immediately to the IT Department so that their network access and email accounts can be suspended or deleted as appropriate immediately.

Abuses of or failure to comply with these arrangements shall result in immediate restriction or disconnection from the network.

Procedures on the restriction of use

Appropriate procedures shall apply in restricting usage after a formal complaint has been lodged or a breach of policy or rule has been reported or detected.

Suspension of the account shall be for a minimum period of four weeks. Formal approval of the relevant Principal and/or the Head of department or Head of section and a signed undertaking to abide by the Rules of Use shall be required before reinstatement of the account.

Permanent disabling of the account shall be taken, where the severity of the offence warrants such action.

3. IT security and internet policy:

Definitions of terms

Spam - Unauthorised and/or unsolicited electronic mass mailings

Chain letters," "Ponzi," "pyramid" schemes- Messages that purport to tell the addressee how, for a relatively small investment, the addressee can make huge amounts of money. There are several variations, but they are all based on a common fraudulent concept — that the addressee pays a relatively small amount of money to a few people above the addressee in a chain, with the expectation that later a very large number of people will be making similar payments to the addressee.

Port scanning- Attempting to learn about the weaknesses of a computer or a network device by repeatedly probing it with a series of requests for information.

Network sniffing -Attaching a device or a program to a network to monitor and record data travelling between computers on the network.

Spoofing -The deliberate inducement of a user or a computer device to take an incorrect action by Impersonating, mimicking, or masquerading as a legitimate source.

Denial of service -Procedures or actions that can prevent a system from servicing normal and legitimate requests as expected.

Ping attack - A form of a denial of service attack, where a system on a network gets "pinged," that is, receives an echo-request, by another system at a fast repeating rate thus tying up the computer so no one else can contact it.

General use and ownership policy

Roles

a) While the IT department is committed to the provision of a reasonable level of privacy, the IT department shall not guarantee the confidentiality of personal information stored or transmitted on any network or device belonging to the Institution. The data created and transmitted by users on the IT systems shall always be treated as the property of the Institution.
b) The IT department shall protect the Institution's network and the mission-critical Institution data and systems. The IT department shall not guarantee the protection of personal data residing on Institution IT infrastructure.
c) Users shall exercise good judgment regarding the reasonableness of personal use of IT services. They shall be guided by IT policies concerning personal use of IT internet, intranet or extranet systems. In the absence of or uncertainty in such policies or uncertainty, they shall consult the relevant IT staff.
d) For security and network maintenance purposes, authorised staff within the IT department shall monitor equipment, systems, and network traffic at any time as provided for in the network and development policy.
e) The IT department shall reserve the right to audit networks and systems periodically to ensure compliance with this IT Policy.

Securing confidential and proprietary information

f) Institution data contained in IT systems shall be classified as either confidential or no confidential. Examples of Confidential Information include but are not limited to payroll data, human resource data, and research data. Employees shall take all necessary steps to prevent unauthorised access to confidential information
g) Users shall keep passwords secure and shall not share accounts. Authorised users are responsible for the security of their passwords and accounts. System-level passwords shall be changed every month; user-level passwords shall be changed at least once every six (6) months.
h) All PCs, laptops, and workstations shall be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host is unattended.

i) Postings by users from the Institution email address to newsgroups shall contain a disclaimer stating that the opinions expressed are strictly the user's and not necessarily those of the Institution unless posting is in the course and within the scope of official duties.

j) All hosts connected to the Institution internet, intranet, or extranet, whether owned by the user or the Institution shall at all times be required to execute approved virus-scanning software with a current virus database.

k) The user shall exercise caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

Conditions of use of computing and network facilities

Unacceptable system and network activities The following activities shall be strictly prohibited, with no exceptions:

Violations of the rights of any person or company protected by India's copyright, trademark, patent, or other intellectual property (IP) law and the Institution's Intellectual Property Policy, other relevant policies, or the Institution's code of conduct.

Introduction of malicious programs into the network or server, for instance, viruses, worms, Trojan horses, or email bombs.

Sharing of the Institution user accounts and passwords– users shall take full responsibility for any abuse of shared accounts

Using the Institution computing resources to actively engage in procuring or transmitting material that could amount to sexual harassment or constitute the creation of a hostile work environment.

Making fraudulent offers of products, items, or services originating from any the Institution account.

Causing a security breach or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which one is not an intended recipient or logging onto a server that one is not expressly authorised to access unless this is within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged attacks, packet spoofing, denial of service, and forged routing information for malicious purposes.

Port scanning or security scanning unless prior notification to IT Department is made.

Executing any form of network monitoring which will intercept data not intended for the originator's host computer, unless this activity is a part of an employee's normal job or duty.

Circumventing user authentication or security of any host, network, or account.

Interfering with or denying service to other network users, also known as a denial of service attack.

Using any program, script, or command, or sending messages of any kind, with the intent to interfere with, or disable, another user's terminal session, via any means, locally or via the internet, intranet or extranet.

Using the Institution network or infrastructure services, including remote connection facilities, to offer services to others within or outside the Institution premises on free or commercial terms.

Wireless network users responsibilities

Any person attaching a wireless device to the Institution network shall be responsible for the security of the computing device and any intentional or unintentional activities arising through the network pathway allocated to the device

The Institution accepts no responsibility for any loss or damage to the user computing device as a result of connection to the wireless network

Users shall ensure that they run up to date antivirus, host firewall, and anti-malware software and that their devices are installed with the latest operating system patches and hotfixes

Users shall authenticate on the wireless network for every session

Wireless network users shall ensure that their computer systems are properly configured and operated so that they do not cause inconveniences to other Institution network users.

The wireless network is provided to support teaching, research, or related academic activities at the Institution. Use of the Institution wireless network services for other purposes is prohibited

Wireless network users shall get their network addresses automatically; a valid network address shall be granted when connected. The use of other network addresses is prohibited.

Appropriate use of electronic mail and communications facilities provided by the Institution are intended for teaching, learning, research, outreach, and administrative purposes. Electronic mail may be used for personal communications within appropriate limits.

Appropriate use and responsibility of users

Users shall explicitly recognise their responsibility for the content, dissemination, and management of the messages they send. This responsibility means ensuring that messages:

- Our courteous and polite.
- Are consistent with Institution policies.
- Protect others' right to privacy and confidentiality.
- Do not contain obscene, offensive or defamatory material.
- Are not used for purposes that conflict with the Institution's interests.
- Do not unnecessarily or frivolously overload the email system (e.g. spam and junk mail).
- Do not carry harmful content, such as viruses.
- Are not for commercial purposes.

4. Email Account Use Policy:

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

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 Institution'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.
- While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
- User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
- User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.
- 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.

5.IT Hardware Installation Policy

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

Who is Primary User:

An individual in whose room the computer is installed and is primarily used by him/her, is considered to be "primary" user. If a computer has multiple users, none of whom are

considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

What are End User Computer Systems

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

Warranty & Annual Maintenance Contract

Computers purchased by any Section/Department/Project should preferably be with 3-year on-site comprehensive warranty. After the expiry of warranty, computers repaired by outside vendor. Such maintenance should include hardware part change, motherboard repair.

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 Institution**

For all the computers that were purchased by the Institution centrally and distributed by the IT Department and will attend the complaints related to any maintenance related problems.

6.User Support Services Policy

Definition of Terms

IT projects: Any IT work or undertaking, and has a clear beginning and end, and is intended to create or deploy IT technology, product, knowledge, or service.

Basic Operation Unit (BOU): A laboratory with or more computers used by academic, non-teaching staff or students for general use, research, in a classroom setting, and operated by an autonomous Department, School, Faculty, Institute, Centre or other Unit of the Institution.

Hardware: All Institution-owned computer and peripheral equipment (such as printers, scanners, CD-ROMS (Read-only memory compact discs, network cards, and multimedia equipment.

Tools and equipment: The stock of shared tools maintained both centrally at the IT department and within individual campuses for use by the support personnel.

IT user support services: IT services directed at IT users to enable them effectively exploit IT technologies, products, and services available at the Institution. These shall mean all activities, carried out by the support personnel involving setup, creation, procurement and acquisition, installation and deployment, repair and training on IT products and services, to assist users in maximising expected utility and benefit

Support coverage: Support site and deployment of support personnel following the assessed support load per site.

Hardware support: Attending to problems associated with hardware categories as listed under the support policy.

Software support: Attending to problems associated with software categories as listed under the support policy.

MIS support: support for corporate Information Systems used by the Institution.

Introduction the IT department acquires, develops and develops a variety of IT technologies, products, and services in response to the academic business and related requirements of the Institution. Upon production, these requirements are distributed (or made available) to users. Thereafter, continuous and tailored support is necessary for users to fully exploit them. A policy guideline is necessary for this support.

Policy Objectives

A guideline for the IT user support service for enabling bona fide Institution IT users to productively exploit provided Institution IT resources.

Specific Services include general user support service; PC and User Peripheral Service; Hardware Maintenance Service; Software Support Service, Network Support Service; IT Staff Professional Training Service; IT User Training Service; Operationalisation of IT Projects.

Policy Scope: This guideline shall steer the activities of producers and consumers of IT technology, products, and services across the Institution.

Institution IT projects and services

The Deputy Director, IT shall ensure that IT Support services are available to assist Institution IT users with technical and logistical support in the implementation (or roll-out) and operationalisation of IT technology, projects, products; and services.

Advocacy: The IT department through user support services shall provide users with consultancy services on IT related matters; it shall provide technical representation in all IT related meetings and committees in colleges and campuses; it shall communicate relevant user support information to users, and provide them with liaison interface (or escalation point) to the IT department.

Support coverage

Support sites shall be designated by campus and to some extent by function. These shall be as detailed in the schedule of support coverage in the standards document

The IT Support function shall provide qualified support personnel at each Institution campus. IT support personnel shall be deployed following the assessed support load per support site (or campus). The load shall be proportional to the extent to which IT s are in use, determined mainly by the expansion of the Institution network and the number of users there off.

Procurement support

The IT user support function shall assist users in deriving the technical requirements and specifications of all IT acquisitions and purchases. Other acquisitions and purchases must meet the minimum specifications as outlined in the IT procurement policy for all hardware, software, services, and consumables to guarantee support by IT under the categories outlined above. The IT user support function shall verify all IT acquisitions and purchases.

Infrastructure support

The IT user support function shall assist users in carrying out surveys, design, requirements specifications, and preparation of BOQs, material acquisition, and supervision of the implementation of all IT infrastructures at the Institution.

Hardware support

The user shall be responsible for daily care and basic routine maintenance of IT hardware under their care as defined in the section on IT equipment maintenance policy.

On a second level, the IT support function shall support the hardware categories that are commonly required by users in their offices, computer rooms, laboratories, and lecture theatres to perform their job responsibilities. These shall include servers, desktop computers, laptop computers, printers, scanners, digital cameras, liquid crystal display (LCD) projectors, network access hardware, among others.

Software and MIS support

IT user support shall support software categories that are commonly required by users for use in their offices, computer rooms, laboratories, and lecture theatres to perform their job responsibilities.

IT Services support

The IT department shall support IT services that are commonly required by users in their offices, computer rooms, laboratories, and lecture theatres to adequately perform their job responsibilities.

Services acquisitions shall meet the minimum specifications as outlined in the IT procurement policy to guarantee support by IT.

Departmental support

The IT support function shall act as the second level support to the existing Computer Laboratory Administrator for Institution Basic Operation Units (BOU). IT department staff shall be available to consult or to help with significant problems.

The IT department shall not be available to provide basic and routine cleaning and simple troubleshooting for machines except where such computer laboratories are directly owned by the IT department

Network devices

The IT department hall own core network active devices such as switches, routers, bridges, gateways and related equipment including enclosures, and shall be responsible for the following:

a) Creating and maintaining an adequate operating environment (floor space, environment control, ventilation, backup power supply) for the equipment.
b) Routine maintenance and upgrade of the equipment.
c) Advising on all expenses incurred during repair, maintenance, and upgrade.

Printing Facilities

A BOU in the Institution may implement a centralised printing facility at which most print jobs shall be processed. This shall be equipped with at least one print device of appropriate specification

Escalation of support requests

Where necessary, the IT support function shall escalate user support requests to appropriate IT department sections and other Institution functional units.

Support resources

The College/Campus/Department shall provide office and workshop space; furniture; and basic office amenities to IT support function.

Tools and Equipment

Every campus shall have a stock of support tools consisting of items as determined by the support work within. Also, a stock of shared tools shall be maintained centrally in the IT department.

Dress and Gear

Support personnel shall be supplied with protective and safety clothing and gear suitable for the tasks involved in the support activities. These shall include items such as overalls, dust coats, dust masks, safety gloves, and other items as the management of the IT department may determine from time to time.

Logistical Resources

Towards realising the set support standards such as turn-around time and low downtime, the IT department shall ensure the availability of logistical resources for transport to ensure rapid movement between support sites and communications to ensure contact between support personnel.

Communication: Support personnel shall be equipped with appropriate communication equipment to maintain effective contact with one another in the course of duty.

Enforcement

The Enforcement of this policy shall be the responsibility of the Deputy Director, IT. This shall be ensured through strict adherence to the IT standards.

Violations will be addressed through established Institution and national legal mechanisms.

Where required and applicable, the Vice-Chancellor shall provide oversights, insights, and guidance in case of any violation.

7. IT Operations and Maintenance Policies

Policy Statement: The YIT is highly dependent on technology to perform its activities daily. As a result, the Institution has adopted a formal approach to operating and maintaining its Information Technology ("IT") systems and resources.

Objective: The objective of this policy is to define the roles, responsibilities, and critical elements for the efficient operations and support of IT systems at the Institution.

This policy applies to:

a) All universities offices, campuses and learning centres, including specifically the IT department.
b) All IT systems or applications managed by the Institution that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.
c) IT Problems" are conditions or situations (known or unknown) that can result in an incident.
d) "IT Incidents" are unplanned events that cause an interruption to, or a reduction in, the quality of the IT operations or services.
e) "Security Vulnerabilities" are IT problems that present specific risks to cybersecurity. Vulnerabilities that have a high probability of being exploited and that will highly impact the Universities (risk of operation disruption, data breach, etc.) are often labelled as "Critical" or "High".

8. End User support:

The IT support team will act as the central point of contact for all IT technical requests.

The users will log the service request with the IT support team by call or mail

The IT help desk will use the following guidelines to prioritise its response to requests

- **Emergency:** Requests for issues having a significant and immediate impact on the Institution's .

For example:

An issue is affecting all or a large number of users.

An issue is preventing users from accessing critical applications or data, or impacting critical functions.

- **High: Requests** for issues having an important impact on the Institution's operations.

For example:

An application error is affecting a small group of users.

An issue is impacting important functions in a system.

An information security incident or vulnerabilities with a medium/high severity/risk.

- **Low :**Requests for issues having a limited or non-immediate impact on the Institution's operations. For example:

An issue is affecting one person only.

An issue is impacting a non-critical function in a system (reporting for example).

A security incident or vulnerability with a low/medium severity/risk.

A "cosmetic" request, to improve a system functionality "look and feel" or a minor non-functional change to a system.

The assigned System administrator or IT assistant will respond to all requests submitted to the IT team within a one- week period where possible. If a request cannot be processed within a one-week timeframe, the System administrator or IT assistant should inform the user who submitted the request.

9. E-waste policy:

E-waste has been defined as-

"Waste electrical and electronic equipment, whole or in part or rejects from their manufacturing and repair process, which are intended to be discarded."
Whereas, electrical and electronic equipment has been defined as
"Equipment which is dependent on electrical currents or electromagnetic fields to fully functional".
Like hazardous waste, the problem of e-waste has become an immediate and long-term concern as its unregulated accumulation and recycling can lead to major environmental problems endangering human health. This calls for an urgent need for e-waste management so as to preserve the ecological balance and reduce landfills. Recycling end-of-life products is vital if we are to save resources and minimise waste.

Do's and Don'ts of E-waste:

Do's:

l) Always look for information on the catalogue with your product for end-of-life equipment handling.

m) Ensure that only authorised recyclers/ dismantler handle your electronic (i.e. LED TV's and accessories) products

n) Always call at your products toll-free no's to dispose of those that have reached the end-of-life.

o) Always drop your used electronic products, batteries or any accessories when they reach the end of their life at your nearest authorised e-waste collection points.

p) Always disconnect the battery from product, and ensure any glass surface is protected against breakage.

Don'ts:

a) Do not dismantle your electronic products on your own.

b) Do not throw electronics in bins having "Do not Dispose" sign.

c) Do not give e-waste to informal and unorganised sectors like Local Scrap Dealer/ Rag Pickers.

d) Do not dispose of your product in garbage bins along with municipal waste that ultimately reaches landfills.

The E-waste collected at the Institution is stocked at the E-waste godown, and is disposed to E-waste handlers – "**Moogambigai Metal Refineries**" who are licensed for processing e-Waste, recycling, and management activities from Karnataka state pollution control board.