YENEPOYA

(DEEMED TO BE UNIVERSITY)
Recognized under Sec 3(A) of the UGC Act 1956
Accredited by NAAC with 'A' Grade

Name of the Policy/ Guidelines	IT Policy
Short Description	Policy and guidelines on IT
Scope	This policy is applicable to Yenepoya (Deemed to be University) and all its constituent colleges and departments
Policy status	Revised
Year of approval of Version 1	2021
Revision	Yes
Effective date	05-04-2021
Approval Authority	53rd Board of Management
Responsible officer	Registrar

RAJESH K. KARKERA
Deputy Director
Information and Communications Technology
Yenepoya (Deemed to be University)
Deralakatte, Mangaluru-575018

Registrar
YENEPOYA
(Deemed to be University)

YENEPOYA
(DEEMED TO BE UNIVERSITY)
Recognized under Sec 3(A) of the UGC Act 1956
Accredited by NAAC with 'A' Grade

University Road, Deralakatte, Mangaluru – 575 018

No. Y/REG/PA/BOM-52/Notification/001/2021 Date: 31.03.2021

NOTIFICATION

Sub: Information Technology Department Policy - reg.
Ref: 53rd meeting of the BoM held on 23.03.2021 – Agenda 7.

.....

As discussed under Agenda 7 of the 53rd Board of Management Online meeting held on 23rd March 2021, it was resolved to approve the Information Technology Department Policy and the same is being notified with effect from 31st March 2021.

Dr. Gangadhara Somayaji K.S.
Registrar

Registrar
Yenepoya (Deemed to be University)
University Road, Deralakatte
Mangalore 575 018

Encl:
Information Technology Department Policy.

To:

Dy. Director, IT

Copy to:
IQAC/Academics.

YENEPOYA

(DEEMED TO BE UNIVERSITY)
Recognized under Sec 3(A) of the UGC Act 1956
Accredited by NAAC with 'A' Grade

INFORMATION TECHNOLOGY DEPARTMENT

POLICY GUIDELINES

Registrar
YENEPOYA
(Deemed to be University)

Table of contents

Sl. No.	Chapter	Page number
	Abbreviations and Acronyms	
1	Introduction to the policy	4
2	Network development and management policy	5
3	IT security and internet policy	15
4	User Support Services Policy	30
5	IT Training Policy	34
6	IT Literacy	34
7	IT Procurement Policy	36
8	IT Operations and Maintenance Policies	38
9	Help desk and User support	38
10	E-waste policy	40
11	Policy to prevent and deal with technology misuse/abuse	41

Abbreviations and Acronyms

1. ATM Automatic Teller Machine
2. BOQs Bill of Quantities
3. BOU Basic Operation Unit
4. BYOD Bring Your Device
5. CDs Compact Discs
6. CD-ROMS Read-only memory compact discs
7. CDRW Read/Write CD
8. DBA Database Administrator
9. DAS Direct Attached Storage
10. DVDs Digital Video Discs
11. FTP File Transfer Protocol
12. GFS Grandfather-Father-Son
13. IT Information Technology
14. IT C Information and Communication Technology Centre
15. IEEE Institute of Electrical and Electronics Engineers
16. IS Information System
17. ISO International Organization for Standardisation
18. IP Internet Protocol
19. IP Intellectual Property
20. IPSec Internet Protocol Security
21. LCD Liquid Crystal Display
22. MIS Management Information System
23. LAN Local Area Network
24. NAS Network Attached Storage
25. NFS Network File System
26. OIC Officer in Charge of Campus
27. PDAs Personal Digital Assistant
28. PSTN Packet-Switched Telephone Network
29. POC Point of Contact (30) SSH Secure Shell
30. SANs Storage Area Networks
31. SLA Service Level agreement
32. SQL Structured Query Language
33. Telnet A terminal emulation program for TCP/IP networks such as the internet
34. TCP Transmission Control Protocol
35. UPS Uninterrupted Power Supply
36. UMIS University Management Information System
37. VPN Virtual Private Networks
38. WAN Wide Area Network
39. Wi-Fi Wireless Fidelity
40. WWW World wide web
41. ZIP "Zip" is the generic file format of a compressed archive

1. Introduction to the policy

1.1 Preamble

Information Technology has been globally recognised as an essential vehicle of "growth and development" in the new millennium. Yenepoya (Deemed to be University) 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 university operation

The University has invested in a strong IT base, which supports teaching, learning, research, and management. The University recognises IT as a prime mover and driver in stimulating creativity and innovation in the current highly technologically driven environment. The strategic role of IT can, therefore, not be gainsaid. The performance and visibility of the University are determined to a great extent by its IT function.

It is against this background that the University has taken the initiative of developing and regularly reviewing a blueprint that will guide in the design, development, implementation, and effective use of the IT services and resources.

1.2 Statement of purpose

The purpose of this IT policy is to outline the acceptable use guidelines for IT equipment and services at the University. 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 University IT infrastructure to ensure efficient and effective use of University 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 University. 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 University;
- 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 University's IT infrastructure;
- Provide a framework, including guidelines, principles, and procedures for the development and implementation of management information systems in the University;

- Guide the handling of organisational information within the IT department and the University 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 university intranet use;
- Uphold the integrity and image of the University through defined standards and guidelines for ensuring that the content of the University'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;

1.3 Scope of the university IT policy

This policy applies to any person accessing/developing/implementing and/or using IT-based Information and IT resources owned, managed, supported, or operated by, or on behalf of, the University. This includes all university staff and students; any other organisations accessing services over University IT resources; persons contracted to develop, repair, or maintain University's IT resources; and suppliers of outsourced IT services. This policy applies to all IT equipment, software, or other facilities that are owned or leased by the University.

Adherence to this policy applies to all these and other relevant parties.

2. Network development and management policy

2.1 Introduction

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

b. The university network functions shall be broken down into the following areas:

- University Infrastructure development

- University backbone
- Campus Local Area Networks (LANs)
- Wireless networks
- Virtual Private Networks (VPN)
- Connection to, access and usage of IT facilities
- New or changed use of IT equipment
- Monitoring of network performance.

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

2.2 Objectives

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

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

2.3 Scope

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

2.4 General network policy

2.4.1 The network

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

2.4.2 Universal availability

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

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

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

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

2.4.3 reliability

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

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

2.5 University IT infrastructure development

2.5.1 Development Plan

The IT will prepare a rolling five (5) year network development plan, advising on appropriate developments aimed at ensuring the adequacy of the University's IT infrastructure in the future. This plan will take account of the University's strategic plan; usage and demand patterns; technological change; security; management, and cost implications.

2.5.2 Implementation of new developments

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

b. 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.

2.5.3 IT network provision in new and refurbished buildings

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

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

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

2.6 University backbone

2.6.1 Definition

The university network will consist of several parts: "Backbone" systems, a collection of inter-building connections; "Campus LANs," wireless networks (Hotspots); Virtual Private Networks (VPN), etc.

The university 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.

2.6.2 Structure of university backbone

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

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

c. Connection to the university network backbone shall be approved by the Deputy Director, IT.

d. The IT Department shall adhere to and maintain copies of all relevant networking standards, and keep abreast of national and international developments in these standards.

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

2.7 Campus LANs

2.7.1 Definition

The respective OICs will take responsibility for the Campus LANs, namely, the necessary wiring and related equipment within existing buildings to allow connection to the LAN gateways.

2.7.2 Structure of campus LANs

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

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

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

d. In cases where there are constraints to connecting any building to the university network, backbone, consultations and subsequent approvals by the Deputy Director, IT shall be made to allow for alternative configurations.

2.8 Inter-campus connections

2.8.1 Definition

The inter-campus connections shall consist of the necessary services and related equipment that allow a remote campus or remote university office to access the central university backbone.

2.8.2 Structure of inter-campus connection

a. Wherever feasible, the network(s) within each remote site will be arranged so that there will be one point of connection to the university network backbone. In cases where it is not possible to establish a single connection, multiple inter-campus connections may be established.

b. Network protocols used on Inter-campus connections must use approved configuration parameters, including approved network identifiers.

c. Inter-campus links connecting to the university network shall meet the university network security and management requirements.

2.9 Wireless networks

2.9.1 Definition

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.

2.9.2 Structure of wireless networks.

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

b. Any request for the installation of a wireless device must be approved by Deputy Director, IT.

c. Wireless access points shall terminate at a point of connection to the university 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.

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

2.10 Virtual Private Networks (VPN)

2.10.1 Definition

Virtual Private Network (VPN) extends university networks across the internet enabling users to send and receive data across shared or public networks as if they are directly connected to the university network while ensuring security and applicable policies are observed.

2.10.2 Structure of Virtual Private Networks

a. Authorised users of University IT services shall be granted rights to use VPN connections if they intend to gain access to the University IT intranet services through public networks.

b. By using VPN technology, users are subject to the same rules and policies that apply while on campus.

c. Users of this service are responsible for procurement and cost associated with acquiring basic Internet connectivity, and any related products or services.

d. It is the responsibility of the user with VPN privileges to ensure that unauthorised users are not allowed access to the university networks through their credentials.

e. All VPN services are to be used solely for the approved university business or academic purpose.

f. All VPN service usage shall be logged and subject to auditing.

g. Network protocols used on VPNs and communicating through the gateway must use approved configuration parameters, including approved network credentials.

2.11 Access to IT facilities

2.11.1 Server Rooms, network racks, and IT network equipment

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

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

c. 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 Deputy Director, IT.

2.11.2 Access in an emergency

a. 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.

b. Where IT network equipment is housed in rooms used for other purposes, the arrangements for access by the other user of the room shall require the prior written consent of the Deputy Director, IT. This consent shall specifically exclude access by the other user to any communications cabinets or IT network equipment located in the shared room.

2.11.3 Contractors

a. Contractors providing IT network services must obtain the prior approval of the Deputy Director, IT and shall obtain the appropriate authorisation in compliance with procedures and regulations of the university security system.

b. Contractors shall observe any specific access conditions which apply within the areas in which they will be working. These access conditions include, in all cases, that contractors working in main server rooms shall be accompanied by appropriate University IT personnel.

2.11.4 Installation of cabling

All installations and changes of electrical power cabling in facilities housing IT equipment shall be approved and managed by the maintenance department in consultation with the Deputy Director, IT in writing.

2.11.5 Installation of equipment

The specification of any equipment to be installed in communications rooms and cabinets and the installation of such equipment shall require the prior written consent of the Deputy Director, IT.

2.11.6 Network equipment

a. 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 University's IT networks.

b. Where the Deputy Director of IT agrees that academic staff or the IT department's technical staff may install and maintain hubs and switches within local staff or student networks, such permission will in every case specifically exclude the point at which these hubs and switches connect to the University's network infrastructure.

2.12 Connection to and usage of IT facilities

2.12.1 Connecting to the IT network

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

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

c. Computer workstations connected to the IT network will not be set up to offer services to other users, for example, to act as servers, unless the prior written consent of the Deputy Director IT has been obtained. Such consent will normally exclude all external access

2.12.2 External access to servers on the backbone network

a. External access means access by a person's external to the University; access to the backbone network from external locations.

b. Where specific external access is required to servers on the backbone network, the Deputy Director IT shall ensure that this access is strictly controlled and limited to specific external locations or persons.

c. The Deputy Director IT will monitor compliance with access arrangements as stipulated in this IT Policy and the relevant IT security policy on server security issued by the University from time to time.

2.12.3 Domain Name Services

All Domain Name Services (DNS) activities hosted within the University shall be managed and monitored centrally, for the whole University, by the IT department.

2.12.4 Suspension and/or termination of access to IT networks

a. A user's access to the University's IT networks will be revoked automatically:

   i. At the end of studies, employment or research contract;

   ii. At the request of the Director/Dean of Faculty/Head of Resource Centre/Head of Department or Head of Unit;

   iii. Where there is a breach of these regulations

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

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

d. 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

a. 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.

b. Any breach of IT policy shall be reported or communicated in writing to the Deputy Director, IT

c. Upon receipt of any such complaint, the Deputy Director, IT shall classify the complaint as "serious" or "non-serious." A "non-serious" complaint shall be defined as a breach of policy which does not subject the University to a cost nor any high risk.

d. When a complaint is classified as "non-serious," the Deputy Director, IT is authorised to impose any one of the following penalties:

   i. Suspension of the account for a minimum period of four weeks.

   ii. Permanent disabling of the account.

e. When a complaint is classified as "serious," the Deputy Director, IT shall refer the complaint to the Vice-Chancellor/Registrar/Deans for appropriate action. The possible penalties may be any one or a combination of the following:

i. Suspension of the account which will be communicated to the relevant Director/Dean and/or Head of Department or Section;

ii. Suspension of the account shall be for a minimum period of four weeks. Formal approval of the relevant Director/Dean 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.

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

iv. Accounts may be reinstated before the end of the suspension period where either the student or staff presents information to the Deputy Director, IT, which indicates that he or she was not involved in the transgression of the rules of use, or the Director/Dean and/or the Head of department or Head of section requests the account be reinstated for employment/course-related work only (e.g. completion of an assignment). In this case, the user is required to sign an undertaking to abide by the Rules of use.

v. A system administrator can make a recommendation to disable an account to the Deputy Director, IT. The Deputy Director, IT, shall review the request. If it is considered to be, on the balance of probability, a transgression of the IT Policy, the account shall be suspended.

vi. Users should note that suspension of access to IT facilities also includes access to the terminal server password access, and as such dial-up modem access will be disabled where a user account is suspended.

2.12.5 Additional or changed equipment

a. The Deputy Director IT shall be advised in advance and at the earliest opportunity, of any plan to add items of desktop services equipment to or to replace or to relocate desktop equipment that is connected or that may require connection to the University's IT network.

b. The Deputy Director IT shall assess the likely impact on the University's IT networks of the proposed change. The Deputy Director IT shall approve the proposed change only where appropriate adjustments can be made to accommodate any effects on network traffic that this change may cause.

2.12.6 External data communications

a. All external data communications shall be channelled through university-approved links.

b. No external network connections shall be made without the prior written consent of the Deputy Director, IT.

c. The installation and use of leased or private links on premises owned, managed, or occupied by the University shall require the prior written consent of the Registrar/Dean.

d. The use of modems, leased or other means of access to other networks on equipment located on premises owned, managed or occupied by the University that are linked to the University IT network infrastructure, is prohibited, unless a proposal and justification for such connection have been authorised in writing by the Deputy Director, IT.

2.12.7 Web filtering

The Deputy Director, IT shall be responsible for the implementation of appropriate filtering facilities for web-based and non-web Internet traffic, including MP3 traffic and other high bandwidth-intensive services that may not have direct educational or research value, where and when necessary in conformity with the IT policy and relevant IT guidelines that promote efficient and high availability of internet services to the majority of users.

2.13 New or changed use of IT equipment

a. The Deputy Director, IT shall be informed in advance of any plan that involves a new use, a change of use or addition to the University's IT networks that might impact on the performance or security of the network.

b. The Deputy Director, IT, shall assess the likely impact of the proposed use and will advise on the consequential impact upon the performance of the University's IT network. Such changes shall be effected after approval by the Deputy Director, IT.

3. IT security and internet policy

3.1 Definitions of terms

a. Spam - Unauthorised and/or unsolicited electronic mass mailings

b. "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.

c. 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.

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

e. 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.

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

g. 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.

3.2 General use and ownership policy

3.2.1 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 University. The data created and transmitted by users on the IT systems shall always be treated as the property of the University.

b. The IT department shall protect the University's network and the mission-critical university data and systems. The IT department shall not guarantee the protection of personal data residing on University 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.

3.2.2 Securing confidential and proprietary information

a. University 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

b. 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.

c. 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.

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

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

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

3.3 Conditions of use of computing and network facilities

3.3.1 Unacceptable system and network activities

The following activities shall be strictly prohibited, with no exceptions:

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

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

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

d. Using the university 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.

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

f. 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.

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

h. 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.

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

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

k. 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.

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

3.3.2 Wireless network users responsibilities

a. Any person attaching a wireless device to the university 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

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

c. 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

d. Users shall authenticate on the wireless network for every session

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

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

g. 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.

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

3.3.3.1 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:

i) Our courteous and polite;

ii) Are consistent with university policies;

iii) Protect others' right to privacy and confidentiality;

iv) Do not contain obscene, offensive or defamatory material;

v) Are not used for purposes that conflict with the University's interests;

vi) Do not unnecessarily or frivolously overload the email system (e.g. spam and junk mail);

vii) Do not carry harmful content, such as viruses

viii) Are not for commercial purposes

3.3.3.2 Confidentiality and Security

a. Electronic mail is inherently NOT SECURE.

b. As the university networks and computers are the property of the University, the University retains the right to allow authorised IT, department staff, to monitor and examine the information stored within.

c. It is recommended that personal confidential material is not stored on or sent through the University IT infrastructure.

d. Users must ensure the integrity of their password and abide by university guidelines on passwords.

e. Sensitive, confidential material shall not be sent through electronic mail unless it is encrypted.

f. Confidential information shall be redirected only where there is a need and with the permission of the originator, where possible.

g. Users shall be aware that a message is not deleted from the system until all recipients of the message and any forwarded or attached copies have deleted their copies.

h. Electronic mail messages can be forged in the same way as faxes and memoranda. If a message is suspect, users shall verify authenticity with the IT Department.

3.3.3.3 User indemnity

Users agree to indemnify the University for any loss or damage arising from the use of the University's email.

3.3.3.4 Limited warranty

The University takes no responsibility and provides no warranty against the non-delivery or loss of any files, messages, or data nor does it accept any liability for consequential loss in the event of improper use or any other circumstances.

3.4 Bring Your Device (BYOD)

a. Employees who prefer to use their personally-owned IT equipment for work purposes must secure corporate data to the same extent as on corporate IT equipment, and must not introduce unacceptable risks (such as malware) onto the corporate networks by failing to secure their equipment.

b. BYOD users must use appropriate forms of user authentication approved by Information Security, such as user IDs, passwords and authentication devices.

c. The following classes or types of corporate data are not suitable for BYOD and are not permitted on PODs:

   i. Anything classified SECRET or CONFIDENTIAL;

   ii. Other currently unclassified but highly valuable or sensitive corporate information which is likely to be classified as SECRET or above;

   iii. Large quantities of corporate data (i.e. greater than 1 GB in aggregate on anyone POD or storage device).

d. The University has the right to control its information. This includes the right to backup, retrieve, modify, determine access, and/or delete corporate data without reference to the owner or user of the device.

e. The University has the right to seize and forensically examine any device within the university premises believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes.

f. Suitable antivirus software must be properly installed and running on all devices.

g. Device users must ensure that valuable corporate data created or modified on the devices are backed up regularly, preferably by connecting to the corporate network and synchronising the data between the device and a network drive or on removable media stored securely.

h. Any device used to access, store or process sensitive information must encrypt data transferred over the network (e.g. using SSL or a VPN)

i. Since IT User support does not have the resources or expertise to support all possible devices and software, devices used for BYOD will receive limited support on a 'best endeavours' basis for academic purposes only.

j. While employees have a reasonable expectation of privacy over their personal information on their equipment, the University's right to control its data and manage devices may occasionally result in support personnel unintentionally gaining access to their personal information. To reduce the possibility of such disclosure, device users are advised to keep their data separate from university data on the device in separate directories, clearly named (e.g. "Private" and "BYOD").

k. Take care not to infringe other people's privacy rights, for example, do not use devices to make audio-visual recordings at work.

3.5 Password policy

3.5.1 Rules

a. All system-level passwords such as root, enable, windows server administration, application administration accounts, shall be changed at least once every month.

b. All user-level passwords such as email, web, and desktop computer shall be changed at least once every six (6) months.

c. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" shall have passwords distinct from all other accounts held by such users.

d. Passwords shall not be inserted into email messages or other forms of electronic communication.

e. Passwords for the university accounts shall not be used for other non-university access such as personal ISP account, Yahoo Mail, and Bank ATM.

f. All passwords shall be treated as sensitive, confidential university information. Users shall not share the university passwords with anyone, including administrative assistants or secretaries.

g. Users shall not use the "Remember Password" feature of applications like Eudora, Outlook, and Netscape Messenger.

h. Users shall not write passwords down and store them anywhere in their offices.

3.5.2 General password construction guidelines computer passwords are used for various purposes at the University. Since very few systems have support for one-time tokens, that is, dynamic passwords that are only used once, all users shall familiarise themselves with the following information on how to select strong passwords.

Poor, weak passwords have the following characteristics:

a. The password contains less than eight characters

b. The password is a word found in English, Hindi or other dictionaries

c. The password is a common usage word such as:

i. Names of family, pets, friends, co-workers, or fantasy characters.

ii. Computer terms and names, commands, site, company, hardware, software.

iii. The words "university", "New Delhi", "Mangalore" or any such derivation.

iv. Birthdays and other personal information such as addresses and phone numbers.

v. Word or number patterns like aaabbb, qwerty, zyxwvuts, or 123321.

vi. Any of the above spelled backward.

vii. Any of the above preceded or followed by a digit such as ecret1, 1secret. Strong passwords have the following characteristics:

a. Contain both upper and lower case characters like a-z, A-Z.

b. Have digits and punctuation characters as well as letters such as 0-9, !@#$%^&*()_+|~=\`{}[]:";'<>?, or /.

c. Are at least eight alphanumeric characters long.

d. Are not words in any language, slang, dialect, or jargon, among others.

e. Are not based on personal information, or names of family, among others. (f) Where an account or password is suspected to be compromised, the affected passwords shall be changed immediately. The IT department shall be

alerted immediately to investigate the incident if it affects critical university information systems or processes.

3.6 Server security policy

3.6.1 Ownership and Responsibilities

Any server deployed on the university IT network shall have an operational group that shall be responsible for its system administration. Operational groups shall monitor configuration compliance and shall implement an exception policy tailored to their environment. Each operational group shall establish a process for changing the configuration guides; if the server is executing critical university systems, this shall involve a final review and approval by the Deputy Director, IT.

a. All servers shall be registered with the IT Department. At a minimum, the following information shall be forwarded:

   i. Contacts of the system administrator

   ii. The physical location of the server

   iii. Hardware and operating system version in use

   iv. Description of functions and applications of the server

b. Configuration changes for servers shall follow the appropriate change management procedures.

3.6.2 General configuration guidelines

a. Server operating systems shall be configured in line with approved IT guidelines.

b. Services and applications that are not used shall be disabled at all times, for instance, NFS, Telnet, and FTP.

c. Access to services shall be logged and protected through access-control methods such as TCP Wrappers where possible.

d. The most recent security patches shall be installed on the systems as soon as practical, the only exception being when an immediate application would interfere with business requirements.

e. Antivirus software shall be installed and configured to update regularly.

f. Trust relationships, such as through NFS, between systems, are a security risk, and these use shall be avoided. No trust relationship shall be used where alternative secure methods of communication are available.

g. User access privileges on a server shall be allocated on "least possible required privilege" terms, just sufficient privilege for one to access or perform the desired function.

h. Super-user accounts such as "root" shall not be used when a non-privileged account can do.

i. If a methodology for secure channel connection is available, that is technically feasible; privileged access shall be performed over secure channels, for instance, encrypted network connections using SSH or IPSec.

j. Servers shall be physically located in an access-controlled environment.

k. It shall be prohibited to operate servers from uncontrolled or easily accessible areas.

3.6.3 Monitoring

a. All security-related events on critical or sensitive systems shall be logged, and audit trails backed up in all scheduled system backups.

b. Security-related events shall be reported to the system administrator in charge of servers, who shall review logs and report incidents to the IT department and the Deputy Director, IT. Corrective measures shall be prescribed as needed. Security-related events include, but are not limited to:

    i. Port-scan attacks

    ii. Evidence of unauthorised access to privileged accounts

    iii. Anomalous occurrences that are not related to specific applications on the host.

3.7 Anti-Virus Policy

a. All computers connected to the University IT network shall run the university standard supported antivirus software, and shall be configured to perform daily full-system and on-access scans.

b. Antivirus software and the virus pattern files shall be kept up-to-date always through scheduled daily automatic updates.

c. Computer laboratory administrators and owners of computers, in consultation with the relevant IT department personnel, shall be responsible for executing required procedures that ensure virus protection on their computers. Computers shall first be verified as virus-free before being allowed to connect to the university network.

d. Once discovered, any virus-infected computer shall be removed from the university network until it is verified as virus-free.

e. The following precautions shall be observed by all users to reduce virus problems. Users shall:

i. Never open any files or macros attached to emails from an unknown, suspicious or untrustworthy source. All such emails shall be deleted immediately and emptied from trash folders.

ii. Delete spam, chain, and other junk emails without forwarding, in compliance with the general use and ownership policy.

iii. Never download files from unknown or suspicious sources.

iv. Avoid direct disk sharing with reading/write access unless this is necessary.

v. Always scan removable media, including diskettes and memory sticks, from unknown sources for viruses before using.

vi. Backup critical data and system configurations regularly and store the data in a safe place.

vii. Not run any applications that could transfer a virus such as an email or file-sharing in a computer where the antivirus software is disabled. Such a computer shall be disconnected from the network.

viii. Periodically check for antivirus updates and virus alerts because new viruses are discovered almost every day.

3.8 VPN Policy

a. Authorised users of University IT services shall be granted rights to use VPN connections if they intend to gain access to the University IT network services while outside the university premises.

b. All VPN access shall be strictly controlled, using either one-time password authentication or a strong passphrase.

c. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic shall be dropped.

d. All computers connected to the University's internal networks via VPN shall use the most up to date antivirus and anti-malware software that is the corporate standard,

e. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the University's network; these machines must be configured and used in compliance with this IT policy.

f. VPN users shall automatically be disconnected from the University's network after thirty minutes of inactivity and the user required to log in again to reconnect back to the network. Pings or other artificial network processes to keep the connection open indefinitely are prohibited.

3.9 Server Rooms

a. Servers shall be housed in a room built and secured for the purpose.

b. The server rooms shall contain an adequate air conditioning system to provide a stable operating environment and to reduce the risk of system crashes due to component failure.

c. No water, rainwater or drainage pipes shall run within or above computer server rooms to reduce the risk of flooding.

d. Where possible the floor within the computer suite shall be a raised false floor to allow computer cables to run beneath the floor and reduce the risk of damage to computer equipment in the case of flooding.

e. Power feeds to the servers shall be connected through the uninterrupted power supply (UPS) and surge protector equipment to allow the smooth shutdown and protection of computer systems in case of power failure.

f. Where possible generator power shall be provided to the computer site to help protect the computer systems in the case of a mains power failure.

g. Access to the server rooms shall be restricted to the authorised IT staff only.

h. All non-IT Departmental staff working within the server room shall be supervised at all times, and the IT management shall be notified of their presence and provided with details of all work to be carried out, at least 24 hours in advance of its commencement.

3.10 Systems Backup Policy

3.10.1 Responsibility

All IT Department sections that operate key university systems shall formulate and implement systematic schedules for performing regular backups on the systems in their custody. The following cadre of staff shall carry full responsibility concerning data backup implementation: The System Administrators and IT Assistants The responsible staff shall arrange to perform backups as scheduled at all times.

The Deputy Director IT shall be the principal backup custodian. Back-ups of critical systems shall be documented with the IT security office and handed over for safekeeping.

All responsible shall take necessary measures to ensure the integrity, confidentiality, and reliability of the back-ups.

3.10.2 Backup window

Backups for online systems shall be carefully scheduled to diminish any perceived degradation on system performance. Hence, backup windows shall be scheduled at specific times of the day where the most minimal interruption on system services is likely. As a rule of thumb, all major backups shall be scheduled to run at night or during weekends; times when demand for system services is expected to be generally low.

3.10.3 Backup inventory file

The IT department shall maintain a backup inventory file, which shall document all backups carried out on critical university systems. This shall provide mechanisms for quick monitoring and tracking of the implementation of scheduled back-ups.

All relevant backups, whether stored in removable backup media and/or on fixed media (hard-disks), shall be recorded in a backup inventory file.

The backup inventory file shall be kept in a safe storage area, under the custody of the IT Department.

3.10.4 Documenting Data Back-Ups

The following information shall be documented for all generated data backups:

a. Date and time the data backup was carried out (dd/mm/yyyy: hh: mm).
b. The name of the system or short description of the nature of the data
c. Extent and type of data backup (files/directories, incremental/full).
d. Backup hardware and software used (computer name, operating system, and version number).
e. Sequence number if any (where multiple removable backup media are used).
f. The physical location of the server and the logical path on file-system to the backup area, when fixed media (hard-disks) are used.
g. Data restoration procedures. This may be a separate booklet or set of guidelines

The above information shall be filed in the backup inventory file. Removable media, besides, must carry proper labels documenting items (a) to (e).

3.10.5 Verification

There shall be a regular audit of all backup media. It is recommended that this exercise be carried out at least once every three months. A complete set of backup media shall be restored, on a temporary location, and then inspected for accurate data reconstruction.

A report on the outcome of the audit shall be generated and recorded in the backup inventory file.

3.10.6 Storage

a. Removable backup media shall be stored in a locked fireproof safe within an access-controlled room.

b. A complete copy of the current removable backup set shall be moved to secure offsite storage once every month.

3.10.7 Data Restoration Procedures

All step-by-step procedures needed to achieve complete data reconstruction and resumption of system operations from backups shall be documented. A hard copy of this document shall be filed in the backup inventory file.

3.10.8 Backup Retention Period and Media Rotation Schedule

The retention period for backup media shall be set in such a manner as to minimise the risk of catastrophic loss of data at reasonable media cost.

The following guide, commonly known as the Grandfather-Father-Son (GFS) method, shall be adopted:

a. Daily backups, known as the Son, shall be carried out on all, or selected days of the week;

b. The last full daily backup in a week, known as the Father, shall be the weekly backup;

c. Daily backups age only for the length of the week, hence the media shall be reused in the coming week;

d. The weekly backups shall be retained for a month and shall be reused during the next month;

e. The last full backup of the month is known as the monthly backup or the grandfather;

f. The grandfather backups become the oldest and shall be retained for a year before the media can be reused.

Backup media must first be tested to guarantee their integrity before re-use. Media re-use must always begin with the oldest set.

3.10.9 Data Archiving

a. IT Department is obliged to maintain archives of data of critical university systems for a time frame that is beyond the normal backup retention period, in case of the future need to refer to the data by the University or authorised Government agencies.

b. For this purpose, in addition to normal backups, responsible staff shall arrange for a special backup scheduled at the close of each financial year for all sensitive data on respective systems.

3.10.10 Backup Media

a. The following backup media are recommended.

i. Fixed computer hard drives. These can be located over the network on a separate computer or, most preferably, on equipment using specialised storage technology such as Direct Attached Storage (DAS), Network Attached Storage (NAS), and Storage Area Networks (SANs). The use of these media is recommended where fast, very frequent, and high capacity backups are required.

3.10.11 Backup Plans

Back-up plans, with the schedule of the general regular backup pattern for the key university systems, shall be documented. The ratified plan shall be authorised by the Deputy Director, IT, and filed in the backup inventory file. Persons responsible for back-ups shall carryout all back-ups as scheduled on the backup plan, but may also stipulate additional event-dependent intervals where necessary.

3.13 Internet usage policy

a. All software used to access the internet shall be part of the university standard software suite or approved under the ISO standard.

b. All users shall ensure that internet access software shall incorporate the latest security updates provided by the vendors.

c. All files downloaded from the internet shall be scanned for viruses using the University's corporate antivirus software suite with the latest virus detection updates.

d. All internet access software shall be configured to use stipulated gateways, firewalls, or proxy servers. Bypassing any of these servers shall be strictly prohibited.

e. Accessed internet sites shall comply with the University's general use and ownership policy.

f. Internet access traffic through the university IT infrastructure shall be subject to logging and review.

g. The university Internet access infrastructure shall not be used for personal solicitations or personal, commercial ventures.

h. All sensitive university materials transmitted over the internet shall be encrypted.

i. Official electronic files shall be subject to the same rules regarding the retention of records that apply to other documents and information or records shall be retained following university records retention schedules.

4. User Support Services Policy

4.1 Definition of Terms

a. 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.

b. 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 University.

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

d. 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.

e. IT user support services: IT services directed at IT users to enable them effectively exploit IT technologies, products, and services available at the University. 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

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

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

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

i. MIS support: support for corporate Information Systems used by the University.

4.2 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 University. 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.

4.3 Policy Objectives

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

b. 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.

4.4 Policy Scope

This guideline shall steer the activities of producers and consumers of IT technology, products, and services across the University.

4.4.1 University IT projects and services

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

4.4.2 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.

4.4.3 Support coverage

i. 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.

ii. The IT Support function shall provide qualified support personnel at each university 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 university network and the number of users there off.

4.4.4 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.

4.4.5 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 University.

4.4.6 Hardware support

i. 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.

ii. 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.

4.4.7 Software and MIS support

i. 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.

4.4.8 IT Services support

i. 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.

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

4.4.9 Departmental support

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

ii. 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

4.4.10 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.

4.4.11 Printing Facilities

A BOU in the University 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

4.4.12 Escalation of support requests

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

4.4.13 Support resources

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

4.4.12 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.

4.4.13 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.

4.4.14 Logistical Resources

a. 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.

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

4.4.15 Enforcement

a. 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.

b. Violations will be addressed through established University and national legal mechanisms.

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

5. IT Training Policy

5.1 Introduction

A variety of products and services are developed or procured by the IT department in response to the business requirements of the University. Upon production, these products and services are distributed (or made available) to users. Thereafter, continuous and tailored training is necessary in order for users to fully exploit them. The policy shall clarify guidelines for such training.

5.2 Policy objective

The objective of this policy is to outline the guidelines applicable when planning for, organising and conducting IT training at the University.

5.3 Scope

a. This policy specifies the general approach to the training of all university staff and students; and any other stakeholders accessing University IT services, as the primary users of IT services.

b. It addresses the training content and methodology for IT users.

6. IT Literacy

All university staff should be literate users of IT services, the level of literacy being in line with the demands of their job functions. Training shall, therefore, focus on building skills in users, making them effective in exploiting IT resources, products, and services.

6.1 Mode of training

a. External IT training shall be organised by the IT department in response to need as may be assessed from time to time when training is not possible within the University.

b. Internal IT user training targeting the university community shall be scheduled continuously and shall be conducted both on the campuses and at the E-Learning centre in the IT department.

6.2 Trainees

a. The IT department shall jointly with user departments nominate trainees for external IT training when the need for such training arises.

b. An Officer in Charge of Campus (OIC) in response to assessed needs shall jointly with the user departments in their campus nominate users and forward the names to the Deputy Director IT. The operating unit shall make the necessary arrangements to facilitate trainees drawn from such units.

6.3 Training resources

The IT department in liaison with the user department shall identify the appropriate trainers for the training as demanded by the needs of the scheduled training.

The IT department jointly with the user departments shall provide necessary resources to facilitate the training

6.4 Training needs and Curriculum development

OICs, Project Leaders, and service developers shall establish IT training needs in liaison with user departments and service consumers. In cases where the IT department is not well placed to train in a given area, the IT department shall identify and recommend appropriate training and work out the requirements of the training.

a. The IT department shall develop curricula for all training, including the development of source material. To this end, the IT Department shall where possible: i) recommend curriculum for all external training ii) provide training materials on-line via the University website iii) conduct on-line assessment tests and examinations

b. Where external training is sourced, the IT department shall jointly with the external training agent, customise the content to meet the training needs of the users.

6.5 Acknowledgement of training

The IT department shall issue certificates on successful completion of training and examination.

7. IT Procurement Policy

7.1 Definition of terms

a. Department: The University is made up of numerous units. These units control their resources and can, therefore, procure goods and services. These include Colleges, Institutes, Schools, Faculties, Academic Departments, Service Departments, Centre, and administrative offices. In this policy, the term department means the procuring entity within the University.

b. IT goods and services: The IT goods and services to be provided by the qualified and selected bidder under the contract (such as the supply of any major hardware, software, or other components of the required Information Technologies specified, or the performance of any related Services, including software development, transportation, installation, customisation, integration, commissioning, training, technical support, maintenance or repair).

c. Technical specifications: A document intended for use in procurement, which clearly and accurately describes the essential and technical requirements for items, materials, information systems or services, including procedures by which it will be determined that the requirements have been met.

d. Emergency: This is a sudden unforeseen crisis usually involving possible negative consequences, requiring immediate action, in this case, undertaking a sudden procurement.

e. Proposal: This is the activity of establishing and assembling all the specifications and cost elements to initiate an acquisition within an agreed scope.

f. Project: This is a series of activities geared toward achieving a defined objective within a specified period of time.

g. Quotation: This will mean a statement of the present going market price for goods or services, including the accompanying terms as provided by the intending supplier.

7.2 The IT department shall provide the following services:

a. Assist the departments in preparation of technical specifications for the purpose of procuring goods and services related to IT whenever the need arises.

b. Assist the purchasing department in cases of emergencies to identify reputable companies or registered providers to reduce any delay in procurement.

c. The procedures shall conform to the University's rules, regulations, and obligations and ensure that projects for various departments are pursued diligently and efficiently. The procedures shall also ensure that the goods and services to be procured meet the following criteria::

    i. Are of satisfactory quality and are compatible with the balance of the project;

    ii. Will be delivered or completed in a timely fashion; and,

    iii. Are priced so as not to adversely affect the economic and financial viability of the project.

7.3 Policy scope

The IT shall assist the departments with the preparation of technical specifications whenever the need arises. The principles of efficiency and effectiveness in the procurement of the goods and services involved shall guide the process. Transparency in the procurement process is essential.

7.4 Policy statements

The following policy statements shall govern the units or entities of the University in the procurement of IT goods and services in:

a. Identification of the needs and the justification for the procurement of goods and services.

b. Development of the technical specification with the help of the IT and ensure the specification are aligned with the latest technology.

c. Adhere to the procurement policy of the University.

d. Comply with the financial regulations of the University.

e. All IT goods and services shall be delivered to the IT wherever it may be from time to time or such other place as may be agreed between the procuring department and IT centre.