



INFORMATION TECHNOLOGY (IT) POLICY

Preface;

Narayana College of Nursing views IT as the medium for ensuring optimum dissemination of knowledge through its academic, non-academic pursuits and administrative service to all the stakeholders for the criterion of a knowledge society by molding the builders of future.

IT policy exists to create, maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established in the college campus. This policy establishes Institution-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the college. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

IT security involves the protection of information assets from accidental or intentional disclosure, modification, or denial at a reasonable cost. Information Technology Management and Services (ITMS) Department at Narayana college of Nursing aims at identifying, providing and maintaining reliable computing facilities, computing network environment, communication facilities and related infrastructure to facilitate education and Research.

Objectives

1. ITMS reserves the right to monitor the usage of the facilities provided therein to maintain a secure computing environment and to abide by the legal norms that exist.
2. In this document, the term "users" shall mean individuals, staff, students, faculty, departments, offices or any other entity which fall under the management of Narayana educational society and Narayana Medical Campus and require any services aforesaid.
3. Users are bound by all the rules and regulations formulated by the Institution from time to time on use of computing facilities provided to them or owned by them.
4. This document is meant for internal circulation and all users shall have access to this document.



A. n. Sree
Principal

NARAYANA COLLEGE OF NURSING
Chinthareddypalem,
NELLORE - 524 003.

pursuits and administrative service to all the stakeholders for the criterion of a knowledge society by moulding the builders of future.

Any user group or department intending to establish connectivity to external data communications network directly should do so after coordinating with ITMS. ITMS shall extend all necessary technical support to user groups or departments who intend to establish such connections to external data communications. All such direct communication networks shall be routed physically or logically through the central network operations centre of ITMS to maintain security to the campus network.

Policy Content;

Provision of network connectivity and maintenance

- ITMS is responsible for providing users with data communications connectivity from their building to all campus-wide network services.
- ITMS is responsible for the design, development, and maintenance of campus-wide network facilities that are used to connect all users, including facilities such as ISDN, leased data links, fiber optic backbone network or any other technologies that may be adopted.
- ITMS will proactively monitor the shared networks to detect problems and will take actions necessary to isolate the cause and correct the problem.
- Personal devices of users shall be connected to the network after registering the same with the ITMS.

LAN and Intranet security;

1. Computer networks are designed to be open systems and facilitate access to networked resources; data applications system security must rely primarily on the proper application system design and network operating system configuration, rather than on secure physical network facilities.
2. ITMS is responsible for maintaining physical security of all network equipment and data communications cabling in campus equipment closets, between buildings and in network hub locations.
3. Users are encouraged to assist ITMS in maintaining the physical security of the network assets installed at their location and to ensure the integrity of all network related services running on their local hosts.
4. ITMS shall take all necessary security measures to protect and secure the device connected to network and avoid compromises. This may include undisclosed administrator level passwords, restricted access to external or internal ports, restriction on installation of system software by the users, etc.



A. Jai
Principal
NARAYANA COLLEGE OF NURSING
Chinthareddypalem,
NELLORE - 524 003.

5. Compromised or problem hosts connected to the network, once identified will be denied access until they are repaired.
6. To ensure network security, ITMS shall monitor all traffic on the network using appropriate software to identify malicious traffic. If malicious traffic is identified, the host that generated or generating the traffic shall be logically or physically disconnected from the network. ITMS shall recommend remedial actions for such devices connected to the network, which may include: removal of malicious software, fully patched Operating Systems; current anti-virus software and virus definitions; secure passwords, personal firewalls, intrusion detection software, etc. ITMS shall provide necessary support to users for the aforesaid actions.
7. ITMS shall also extend support to users connecting their personal devices to the campus network but limited to the operational or legal constraints.

Provision of network services

3. ITMS shall host all necessary network services to support the activities of the users. This shall include internet connectivity, email services, ftp servers, DNS, DHCP, etc. 2 These services are provided for the purpose of increasing the job fulfillment, job performance, and to increase the productivity.
4. Users shall fill up necessary application forms and secure approval from competent authorities to access services hosted by ITMS.
5. Users shall not divulge passwords, software license codes or other security codes allotted to them to third party. Users are encouraged to reset their passwords every 90 days to ensure access security. All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.
6. Users shall not use MBCET network services to view, download, save, receive, or send material related to or including:
 - Offensive content of any kind, including pornographic material
 - Promoting discrimination based on race, gender, national origin, age, marital status, sexual orientation, religion or disability.
 - Threatening or violent behavior.
 - Illegal activities.
 - Commercial messages.
 - Messages of a political or racial nature.




A. Sune
Principal
NARAYANA COLLEGE OF NURSING
Chinthareddypalem,
NELLORE - 524 003.

- Personal financial gain.
 - Forwarding e-mail chain letters.
 - Spamming e-mail accounts from MBCET's e-mail services or computers.
 - Material protected under copyright laws.
 - Sending business-sensitive information by e-mail or over the Internet.
 - Dispersing organizational data to non-MBCET personnel without authorization.
 - Opening files received from the Internet without performing a virus scan.
 - Recreational streaming of internet material, such as radio, video, TV, or stock tickers.
 - Downloading and/or installing programs/software on any network computer(s) without authorization from the ITMS.
7. ITMS may shutdown the network services periodically for maintenance purposes. Users shall be informed well in advance regarding such outages.
 8. Information regarding such maintenance schedules shall be sent to users through available means of communication which may include but not limited to emails, instant messaging apps or hard copy circulars.

IX Network activities not permitted over the campus network

13. Execution of software programs which excessively consume network or network server resources.
14. Activities that violate rules of local administration, the State, Central Government or recognized International Organization or Treaties.
15. Activities that interfere with the legitimate function of other devices connected to campus network. (examples include DHCP Servers, devices running RIP, RAS Servers consuming DHCP Addresses which have not been registered with ITMS, etc.)
16. Configuring mail servers with open relays, sending unsolicited mails, commercial mails, spamming.
17. Downloading large files for personal use including music, video and software.
18. Probing, scanning or other activities that amount enumeration of campus network.




 Principal
 NARAYANA COLLEGE OF NURSING
 Chinthareddypalem,
 NELLORE - 524 003.

19. Initiating Denial of Service Attacks, Hacking, Cracking or similar activities which disrupt the network services hosted internally and externally.
20. Executing network related software for packet sniffing, content sniffing.
21. Unauthorized access to internal or external network services, devices, servers, or hosts.
22. Illegal distribution of any copyrighted material.
23. "Stealing" or "Borrowing" IP addresses.
24. Any activity that tarnishes MBCET's professional image. (ITMS may not be the policing agency in these matters)

Roles and Responsibilities

1 Key roles and responsibilities for the protection of Institutional Information and IT Resources are listed below. Responsibilities range in scope from the protection of one's own password to security controls administration for a large system or an entire Unit.

Revision

Proposed revisions of this policy should be reviewed by a committee which shall include:

- Principal
- Vice Principal
- Head – ITMS
- One external expert



A. Sare
Principal

NARAYANA COLLEGE OF NURSING
Chinthareddypalem,
NELLORE - 524 003.