MBCET Information Technology (IT) services strives to provide ubiquitous, secure, and seamless access to information resources in all forms and to provide exceptional support to students, faculty, and staff in their endeavours, through a reliable and robust IT infrastructure using the state-of-the-art technologies.

1. OBJECTIVES

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.

2. SCOPE

Information Technology Management and Services (ITMS) Department at MBCET aims at identifying, providing, and maintaining reliable computing facilities, computing network environment, communication facilities and related infrastructure to facilitate education, research, instructional and Institute approved business services. This policy is intended for students, ~~faculty,~~ staff, vendors, and visitors of MBCET.

3. DEFNITION OF TERMS

LAN – Local Area Network
DNS – Domain Name System
DHCP – Dynamic Host Control Protocol
USB – Universal Serial Bus
RS232 – Recommended Standard
IEEE – Institute of Electrical and Electronic Engineers

4. POLICY STATEMENT

4.1 Acceptable IT Devices

4.1.1   Any computer, peripheral or network capable device connected to campus network must belong to, or be formally registered, or be hosted by ITMS.

Prepared By	Approved By	Issued By
Name :	Name :	Name :
DSGN :	DSGN :	DSGN :

4.1.2   ITMS reserves the right to restrict access otherwise.

4.2 Acceptable user behaviour

All users shall

4.2.1   Comply to existing federal, state and, other applicable laws.

4.2.2   Follow copyright laws regarding protected commercial software or intellectual property.

4.2.3   Abide government, telecommunications and networking laws and regulations.

4.2.4   Honour acceptable computer use policy of computer networks accessed through MBCET's campus network either locally or remotely.

4.2.5   Be sensitive to resource utilization and help to provide fair distribution of computer resources by minimizing unnecessary network traffic that may interfere with the ability of others to make effective use of campus network resources.

4.2.6   Obtain prior approval from ITMS before plugging in any additional peripherals to the LAN. This is also applicable to connect peripherals to external ports like USB, RS232, IEEE1394 etc.

4.2.7   Ensure data availability and security by taking regular backups of the data stored on their systems.

4.2.8   Not use MBCET network services to view, download, save, receive or send material related to or including:

   i.   Offensive content of any kind, including pornographic material.
   ii.   Promoting discrimination based on race, gender, national origin, age, marital status, sexual orientation, religion or disability.
   iii. Threatening or violent behaviour.
   iv.   Illegal activities.
   v.   Commercial messages.
   vi.   Messages of a political or racial nature.
   vii. Gambling.
   viii. Personal financial gain.
   ix.   Forwarding e-mail chain letters.
   x.   Spamming e-mail accounts from MBCET's e-mail services or computers

Prepared By	Approved By	Issued By
Name :	Name :	Name :
DSGN :	DSGN :	DSGN :

    xi.   Material protected under copyright laws.

    xii.   Dispersing organizational data to non-MBCET personnel without authorization.

    xiii.   Recreational streaming of internet material, such as radio, video, TV, or stock tickers.

    xiv.   Tampering with ~~your~~ MBCET domain e-mail ID to misrepresent yourself and MBCET to others.

4.3 Provision of computing resources

4.3.1   ITMS shall provide all necessary software for operating the devices allocated to the user.

4.3.2   ITMS reserves the right to secure the administrative passwords for all the devices owned by the Institute.

4.3.3   Users may install any software on the equipment allotted to them after obtaining prior approval from ITMS. ITMS shall reserve the right to restrict users from installing any software that may pose a risk to the security and integrity of the equipment and the campus network.

4.3.4   All software installed on the user machines shall be legal copies from the original vendors. Users are encouraged not to use any illegal or unlicensed versions of copyrighted software.

4.3.5   ITMS shall ensure reinstallation of system and application software if required. Users shall request for the same through facilities provided for making such support requests.

4.3.6   Users shall not copy, duplicate, or distribute any software owned by the College or downloaded by them to their PCs.

4.3.7   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 leased data links, fiber optic backbone network or any other technologies that may be adopted.

4.3.8   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.

4.3.9   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.

Prepared By	Approved By	Issued By
Name : DSGN :	Name : DSGN :	Name : DSGN :

4.3.10 ITMS may shutdown the network services periodically for maintenance purposes. Users shall be informed well in advance regarding such outages.

4.4 Network activities not allowed

4.4.1 Execution of software programs which excessively consume network or network server resources.

4.4.2 Activities that violate local administration, state, central government or recognized international organization or treaties.

4.4.3 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.)

4.4.4 Configuring mail servers with open relays, sending unsolicited mails, commercial mails, spamming.

4.4.5 Downloading large files for personal use including music, video and software.

4.4.6 Initiating Denial of Service Attacks, Hacking, Cracking or similar activities which disrupt the network services hosted internally and externally.

4.4.7 Executing network related software for packet sniffing, content sniffing.

4.4.8 Unauthorized access to internal or external network services, devices, servers, or hosts.

4.4.9 Illegal distribution of any copyrighted material.

4.4.10 "Stealing" or "Borrowing" IP addresses.

4.4.11 Any activity that tarnishes MBCET's professional image.

4.5 Violations

4.5.1 Violations will be reviewed on a case-by-case basis.

4.5.2 If it is determined that a user has violated one or more of the above use regulations, that user will receive a reprimand from his or her Head of the Department or reporting authority and his or her future use will be closely monitored.

4.5.3 If a gross violation has occurred, management will take immediate action. Such action may result in losing Internet and/or e-mail privileges, severe reprimand, and or disciplinary action.

Prepared By	Approved By	Issued By
Name :	Name :	Name :
DSGN :	DSGN :	DSGN :

4.5.4   During the investigation of an alleged policy violation, a user's computing and network access may be suspended.

4.5.5   The decision of the management shall be final and binding on the constituents in case of any conflict or dispute.

5. RESPONSIBILITY

To effectively manage the IT infrastructure facilities and to provide quality IT services to the institution, the structure of ITMS consists of the following subdivisions.

Subdivisions:

1. Network Administration
2. Systems/Server Administration
3. Software Development
4. Client System/Devices Support

Roles:

1. Head – IT Management and Services
2. Systems Administrator
3. Network Administrator
4. System Analyst
5. Programmer
6. Systems Support Technician

Policy Review Committee/Co-ordinator shall review/schedule review of the policy as and when required.

6. RELATED PROCEDURES AND OTHER DOCUMENTS

i.   Password Policy

ii.   Accepted Computer Use Policy (ACUP)

7. POLICY HISTORY

Version/Date	Prepared by	Approved by	Remarks
V0.0/			
V0.1/			

Prepared By	Approved By	Issued By
Name : DSGN :	Name : DSGN :	Name : DSGN :