BETHLAHEM INSTITUTE OF ENGINEERING, KARUNGAL

IT POLICY

CONTENTS

CHAPTER 1 - NEED FOR IT POLICY

1.1 The institute IT policy exists to maintain secure and ensure legal and appropriate use of Information Technology infrastructure established by the institute on the campus.

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

1.3 IT Policy is being documented for fair and transparent academic purpose for use of various IT resources in the Campus for Students, Faculty, Staff, Management and Visiting Guests and Research Fellowship Members.

1.4 BIOE has network connections to every computer system covering all the buildings in the campus and hostel.

1.5 Admin Center is the department that has been given the responsibility of running the institute's intranet and Internet services. Admin Center is running the /firewall security, DHCP, DNS, email, web and application servers and managing the network of the institute.

1.6 When computer systems are networked, viruses that get into the LAN, through Intranet/Internet spread rapidly to all other computers on the net, exploiting the vulnerabilities of the operating systems.

1.7 Too many concurrent users, who are on the high-speed LANs trying to access Internet resources through as limited bandwidth, definitely create stress on the Internet bandwidth available.

1.8 Every download adds to the traffic on the Internet. This adds to costs and after a point, brings down Quality of Service and Quality of Experience. Reducing Internet traffic is the answer.

1.9 Computer viruses attach themselves to files, spread quickly when files are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise.

1.10 Containing a virus once it spreads through the network is not an easy job. Plenty of man-hours and possibly data are lost in making the network safe once more. So, preventing it at the earliest is crucial. Hence, in order to securing the network, Admin Center has been taking appropriate steps by

installing firewalls, access controlling and installing virus checking and content filtering software at the gateway.

1.11 Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

CHAPTER 2 - CLASSIFICATION OF IT POLICIES

- IT Hardware Installation Policy
- Software Installation and Licensing Policy
- Network (Intranet & Internet) Policy
- E-mail Account Policy
- Web Site Hosting Policy
- University Database Policy

2.1 Further, the policies will be applicable at two levels:

- End Users Groups (Faculty, Students, Senior Administrators and other Staff)
- Network Administrators

2.2 It may be noted that institute IT Policy applies to technology administered by the institute centrally or by the individual departments, to information services provided by the institute administration, or by the individual department, or by individuals of the institute community, or by authorized resident or non-resident visitors on their own hardware connected to the institute network.

2.3 This IT policy also applies to the resources administered by the central administrative departments such as Library, Network Admin Centres, Laboratories, Offices and hostels.

2.4 Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the Institute's Information Technology infrastructure, must comply with the guidelines.

2.5 Certain violations of IT policy laid down by the member may even result in disciplinary action against the offender by the institute authorities. If the matter involves illegal action, law enforcement agencies may become involved. Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Applies to

2.6 Stake holders on campus or off campus

- Students: UG, PG, Research
- Employees (Permanent/Temporary/Contractual)
- Faculty
- Administrative Staff (Non-Technical/Technical)
- Higher Authorities and Officers
- Guests

2.7 Resources

- Network Devices wired/wireless
- Internet Access
- Official Websites, Web applications
- Official Email services
- Data Storage
- Mobile/ Desktop / server computing facility
- Documentation facility (Printers/Scanners)
- Multimedia Contents

CHAPTER 3 - IT HARDWARE INSTALLATION POLICY

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

3.1 PRIMARY USER

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

3.2 END USER COMPUTER SYSTEMS

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

3.3 WARRANTY & ANNUAL MAINTENANCE CONTRACT

Computers purchased by any Department/Cells should preferably be with 3-year on- site comprehensive warranty. After the expiry of warranty, computers would be maintained by

Admin Centers or by external Service Engineers on call basis. Such maintenance should include OS re-installation and checking virus related problems also.

3.4 POWER CONNECTION TO COMPUTERS AND PERIPHERALS

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

3.5 NETWORK CABLE CONNECTION

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

3.6 FILE AND PRINT SHARING FACILITIES

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

3.7 MAINTENANCE OF COMPUTER SYSTEMS PROVIDED BY THE INSTITUTE

For all the computers that were purchased by the institute centrally and distributed by the Admin Centers will attend the complaints related to any maintenance related problems.

3.8 NONCOMPLIANCE

BIOE faculty, staff, and students not complying with this computer hardware installationpolicy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computer resulting in loss of productivity. An individual's non- compliant computer can have significant, adverse effects on other individuals, groups, departments, or even whole institute. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

3.9 ADMIN CENTRES INTERFACE

Admin Centers upon finding a non-compliant computer affecting the network will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/phone. The individual users will follow-up the notification to be certain that his/her computer gains necessary compliance. The Admin Centerswill provide guidance as needed for the individual to gain compliance.

CHAPTER 4 - SOFTWARE INSTALLATION AND LICENSING POLICY

Any computer purchases made by the individual departments/cells should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed. Respecting the anti-piracy laws of the country, Institute

IT policy does not allow any pirated/unauthorized software installation on the institute owned computers and the computers connected to the institute campus network. In case of any such instances, institute will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

4.1 OPERATING SYSTEM AND ITS UPDATING

Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them.

4.2 ANTIVIRUS SOFTWARE AND ITS UPDATING

Computer systems used in the institute should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained.

4.3 BACKUPS OF DATA

Individual users should perform regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible. Preferably, at the time of OS installation itself, one can have the computer's hard disk partitioned into many volumes typically C, D and so on. OS and other software should be on C drive and user's data files on the other drives (e.g. D, E). In case of any virus problem, generally only C volume gets corrupted.

In such an event formatting only one volume, will protect the data loss. However, it is not a fool proof solution. Apart from this, users should keep their valuable data on CD / DVD or other storage devices such as pen drives, external hard drives.

4.4 NONCOMPLIANCE

BIOE faculty, staff, and students not complying with this computer security policy leave themselves and others at risk of virus infections which could result in damaged or lost files inoperable computer resulting in loss of productivity risk of spread of infection to others confidential data being revealed to unauthorized persons. An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even whole institute. Hence it

is critical to bring all computers into compliance as soon as they are recognized not to be.

4.5 ADMIN CENTERS INTERFACE

Admin Centers upon finding a non-compliant computer will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/phone. The individual users will follow-up the notification to be certain that his/her computer gains necessary compliance. The Admin Centers will provide guidance as needed for the individual to gain compliance.

CHAPTER 5 - NETWORK (INTRANET & INTERNET) USE POLICY

Network connectivity provided through an authenticated network access connection or Wi-Fi is governed under the Institute IT Policy. The Admin Centers is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the Institute's network should be reported to Admin Centers.

Any computer (PC/Server) that will be connected to the institute network should have an IP address assigned by the Admin Centers. Departments should follow a systematic approach, the range of IP addresses that will be allocated to each building / V LAN as decided.

So, any computer connected to the network from that building will be allocated IP address only from that Address pool.

Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.

As and when a new computer is installed in any location, the concerned user has to take IP address allocation from Admin Centers / respective department.

An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports.

5.1 DHCP AND PROXY CONFIGURATION BY INDIVIDUAL DEPARTMENTS /CELLS/ USERS

Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the institute. Similarly, configuration of proxy servers should also be avoided, as it may interfere with the service run by Admin Centers. Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.

5.2 RUNNING NETWORK SERVICES ON THE SERVERS

Admin Centers takes no responsibility for the content of machines connected to the Network, regardless of those machines being Institute or personal property. Admin Centers will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance. Institute network and computer resources are not to be used for personal /commercial purposes. Network traffic will be monitored for security and for performance reasons at Admin Centers. Impersonation of an authorized user while connecting to the Network is in direct violation of this agreement and will result in the termination of the connection.

5.3 DIAL-UP/BROADBAND CONNECTIONS

Computer systems that are part of the Institute's campus-wide network, whether institute's property or personal property, should not be used for dial-up/broadband connections, as it violates the institute's security by way of bypassing the firewalls and other network monitoring servers. Non-compliance with this policy may result in withdrawing the IP address allotted to that computer system.

5.4 WIRELESS LOCAL AREA NETWORKS

This policy applies, in its entirety, department, or hostel wireless local area networks. In addition to the requirements of this policy, departments, or hostels must register each wireless access point with Admin Centers including Point of Contact information.

CHAPTER 6 - EMAIL ACCOUNT USE POLICY

In an effort to increase the efficient distribution of critical information to all faculties, staff and students, and the Institute's administrators, it is recommended to utilize the institute's e-mail services, for formal Institute communication and for academic & other official purposes. Email for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals.

Formal Institute communications are official notices from the Institute to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general Institute messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging on to https://bethlahem.org with their User ID and password. For obtaining the institute's email account, user may contact Admin Centers for email account and default password by applying in a prescribed proforma.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

- The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- Using the facility for illegal/commercial purposes is a direct violation of the institute's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
- User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender, about its authenticity before opening it. This is very much essential from the point of security of the user's computer; as such messages may contain viruses that have potential to damage the valuable information on your computer.

- User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
- While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
- Impersonating email account of others will be taken as a serious offence under the institute IT security policy.
- It is ultimately each individual's responsibility to keep their e-mail account free from violations of institute's email usage policy. The above laid down policies are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.com etc., as long as they are being used from the institute's campus network, or by using the resources provided by the institute to the individual for official use even from outside.

CHAPTER 7 - WEB SITE HOSTING POLICY

7.1 OFFICIAL PAGES

Departments, Cells, central facilities may have pages on BIOE's official Web Site.

As on date, the Admin Centers is responsible for maintaining the official web site of the institute viz., https://bethlahem.org/

7.2 PERSONAL PAGES

It is recognized that each individual faculty will have individual requirements for his/her pages. Hence, faculty may have their personal pages linked to official web site of the institute by sending a written request or mail to Admin Centers giving the details of the hyperlink of the URL that he/she wants to be added in the official web site of the institute.

However, illegal or improper usage will result in termination of the hyperlink. The contents of personal pages must not violate any applicable export laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial purposes, must not be used for political lobbying, and must not otherwise violate any local state, or central government

laws. Personal pages also will not include the hosting of pages for other individuals or groups.

7.3 RESPONSIBILITIES FOR UPDATING WEB PAGES

Departments, cell, and individuals are responsible to send updated information time to time about their Web pages to Admin Centers.

CHAPTER 8 - INSTITUTE DATABASE USE POLICY

8.1 This Policy relates to the databases maintained by the institute. Data is a vital and important Institute resource for providing useful information. Its use must be protected even when the data may not be confidential. BIOE has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the institute's approach to both the access and use of this institute resource.

8.2 Database Ownership:

BIOE is the data owner of the entire Institute's institutional data generated in the institute.

8.3 Data Administrators:

Data administration activities outlined may be delegated to some of the officers in that department.

8.4 MIS Components:

For the purpose of Management Information System requirements of the institute these are:

- Employee Information Management System.
- Students Information Management System.
- Financial Information Management System.
- Library Management System.
- ocument Management & Information Retrieval System.

8.5 Here are some general policy guidelines and parameters for departments, cells and administrative department data users:

8.6 The institute's data policies do not allow the distribution of data that is identifiable to a person outside the institute.

8.7 Data from the Institute's Database including data collected by departments or individual faculty and staff, is for internal institute purposes only.

8.8 One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies, the institute makes information and data available based on those responsibilities/rights.

8.9 Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office.

8.10 Requests for information from any courts, attorneys, etc. are handled by the Office and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office for response.

8.11 Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to:

8.12 Modifying/deleting the data items or software components by using illegal access methods.

8.13 Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.

8.14 Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.

8.15 Trying to break security of the Database servers.

CHAPTER 9 - HOSTELS WI-FI USE POLICY

Usage of Wireless infrastructure in hostels is to enhance the accessibility of internet for academic purposes and to browse exclusive online resource (licensed online journals) for student's/faculty members and staffs. Availability of the signal will vary from place to place. The signal strength also may vary from location to location. It is not mandatory that each and every area in each floor of every block will have the same kind of signal strength, coverage and throughput.

Access to Wireless internet is only an extended service and neither students nor anyone who is residing in the hostels can demand the service. Availability of wireless services solely depends on the discretion of the institute and it has rights to stop/interrupt the services at any given point of time, if required for any technical

purpose. The access points provided in hostels are the property of institution and any damage or loss of the equipment will be considered as a serious breach of BIOE's code of conduct and disciplinary action will be initiated on the student/s who are found guilty for the loss or damage of the Wireless Infrastructure or the corresponding equipment in the hostel's buildings. In the incident of any loss or damage to the wireless infrastructure, BIOE Admin centre will assess the damage and the same will be recovered from all the students who are residing in that floor/building/hostel.

9.1 RESPONSIBILITIES OF ADMIN CENTERS

a) Campus Network Backbone Operations

1. The campus network backbone and its active components are administered, maintained and controlled by Admin Centers.
2. Admin Centers operates the campus network backbone such that service levels are maintained as required by the Institute Departments, and hostels served by the campus network backbone within the constraints of operational best practices.

b) Maintenance of Computer Hardware & Peripherals MIS Components:

For the purpose of Management Information System requirements of the institute these are:

- Employee Information Management System.
- Students Information Management System.
- Financial Information Management System.
- Library Management System.
- Document Management & Information Retrieval System.

Here are some general policy guidelines and parameters for departments, cells and administrative department data users:

1. The institute's data policies do not allow the distribution of data that is identifiable to a person outside the institute.

2. Data from the Institute's Database including data collected by departments or individual faculty and staff, is for internal institute purposes only.

3. One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies, the

institute makes information and data available based on those responsibilities/rights.

4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office.
5. Requests for information from any courts, attorneys, etc. are handled by the Office and departments should never respond to requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office for response.
6. Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to:
   - Modifying/deleting the data items or software components by using illegal access methods.
   - Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
   - Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.

Admin Centers provides Net Access IDs and email accounts to the individual users to enable them to use the campus-wide network and email facilities provided by the institute upon receiving the requests from the individuals on prescribed proforma.

Disconnect Authorization

Admin Centers will be constrained to disconnect any Department, or cell, hostel from the campus network backbone whose traffic violates practices set forth in this policy or any network related policy. In the event of a situation where the normal flow of traffic is severely degraded by a Department, or cell, hostel machine or network,

Admin Centers endeavours to remedy the problem in a manner that has the least adverse impact on the other members of that network. If a Department or division is disconnected, Admin Centers provides the conditions that must be met to be reconnected.

9.2 RESPONSIBILITIES OF DEPARTMENT

a) User Account

When accessing the institute's computer systems, network, mail and web services and other technological facilities, that Department/End user is personally responsible and accountable to the institute for all the actions performed using that user machines. Hence, users are advised to take reasonable measures such as using complex passwords, not sharing the passwords with others, not writing down the password at a place which is accessible to others, changing the passwords frequently and keeping separate passwords for email account ID to prevent un-authorized use of their user account by others.

It is the duty of the user to know the IT policy of the institute and follow the guidelines to make proper use of the institute's technology and information resources. It is the duty of the user to know the IT policy of the institute and follow the guidelines to make proper use of the institute's technology and information resources.

b) Supply of Information by Department, or Cell for Publishing on /updating the BIOE's Web Site

All Departments or Cells should provide updated information concerning them periodically (at least once in a month or earlier). Hardcopy or softcopy to be sent to the Admin Centers. This policy is applicable even for advertisements/Tender notifications published in newspapers, and the events organized by Department, or Cells. Links to any web pages that have to be created for any specific purpose or event for any individual department or faculty can be provided by the Admin Centers upon receiving the written requests.

If such web pages have to be directly added into the official web site of the institute, necessary content pages (and images, if any) have to be provided by the respective department or individual in a format that is exactly compatible with the existing web design/format. Further, such requests along with the soft copy of the contents should be forwarded to the In Charge, Admin Centers well in advance.

c) Security

In connecting to the network backbone, department agrees to abide by this Network Usage Policy under the Institute IT Security Policy. Any network security incidents are resolved by coordination with a Point of Contact (POC) in the

originating department. If a POC is not available to contact, the security incident is resolved by disconnecting the offending computer from the network till the compliance is met by the user/POC.

d) Preservation of Network Equipment and Accessories

Routers, Switches, Fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries that are installed at different locations by the institute are the property of the institute and are maintained by Admin Centers and respective departments. Tampering of these items by the department or individual user comes under violation of IT policy.

e) Additions to the Existing Network

In addition to the above suggestions, Admin Centers recommends a regular backup strategy. It should be noted that even with all the procedures listed above; there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

CHAPTER 10 - VIDEO SURVEILLANCE POLICY

The system comprises: Fixed position cameras; Monitors; digital video recorders; Storage; Public information signs. Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV Camera installation is in use. Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Purpose of the system

The system has been installed by institute with the primary purpose of reducing the threat of crime generally, protecting institutes premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

It is recognized that members of institute and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Admin Centers. CCTV footage provided by the institute (Admin Centers) upon receiving the requests from the individuals on prescribed proforma.