B. V. V. Sangha’s
Basaveshwar Engineering College (Autonmous)
Bagalkot – 587102, Karnataka, India

IT Policies

(Released on: August 2018, Version 1.0)

Prepared by

BEC Campus LAN Team
Basaveshwar Engineering College (Autonmous)
Bagalkot – 587102, Karnataka, India

Table of Contents

1. Need for IT Policy

Basaveshwar Engineering College (Autnomus), Bagalkot hereinafter referred to as "BEC" Information Technology (IT) policy exists to maintain, secure, and ensure legal and appropriate use of IT infrastructure established. This policy establishes BEC strategies and responsibilities for protecting the confidentiality, integrity, and availability of the information assets that are accessed, created, managed, and/or controlled. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

Realizing the need of Intranet & Internet services in educational institutions & research organizations, BEC took initiative way back in 2000 and established network infrastructure. Now, BEC has around 1500 wired network connections, nearly 75 wireless access points with approximate 3 Kms OFC backbone, managed CISCO switches, wireless access point (WAP) controller, DHCP server, CISCO core router along with the protection from firewall. BEC Campus LAN is the unit that has been given the responsibility of running the BECIntranet & Internet services. BEC is getting its Internet bandwidth from Internet Service Provider (ISP) BSNL. Bandwidth availability is through Internet Leased Line (ILL – 1:1) with 100 Mps.

Due to network challenges/issues such as prolonged or intermittent surfing, heavy downloads that lead to choking of available bandwidth, sexual harassment due to harmful and embarrassing content, confidential information being made public, etc., BEC proposes to have its own IT Policy that works as guidelines for using the BEC computing facilities including computer hardware, software, E-mail, information resources, Intranet and Internet access facilities, collectively called "Information".

These guidelines provide a balance between security and the ability to conduct the rightful functions by the users. Due to the dynamic nature of the Information Technology, Information security is in general and therefore policies that govern information security process are also dynamic. They need to be reviewed periodically and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

Proposed IT Policy applies to BEC administration, individual departments, individuals of BEC, authorized resident and non-resident visitors on their own hardware connected to the BEC network. IT policy also applies to the central administrative departments such as Library, Computer Centers, Laboratories, Offices, Hostels, Guest houses and staff quarters wherever the network facility was provided. Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the IT policy. Certain violations of IT policy laid down by the BEC may result in disciplinary action against the offender by the BEC authorities. If the matter involves illegal action, law enforcement agencies may become involved.

IT policies may be classified into following groups:

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

2. IT Hardware Installation

This section presents BEC IT hardware installation policy which helps 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.

2.1 If a computer has multiple users, none of whom are considered the "primary" user (an individual in whose room the computer is installed and is primarily used by him/her, is considered to be “primary” user), the department or section head should make an arrangement and make a person responsible for compliance.

2.2 Apart from the client PCs used by the users, BEC will consider servers not directly administered by BEC Campus LAN, as end-user computers. If no primary user can be identified, the department or section 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 BEC Campus LAN, are still considered under this policy as "endusers" computers.

2.3 Computers purchased by any Section/Department/Project should preferably be with 3-year onsite comprehensive warranty. After the expiry of warranty, computers are to be under annual maintenance contract. Such maintenance should include hardware failure, performance degradation, etc.

2.4 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. Wherever possible usage of generators are encouraged during long time power failure.

2.5 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.

2.6 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.

2.7 Computer system may be moved from one location to another with prior written intimation to the BEC Campus LAN, as it maintains a record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building name abbreviation and room No. As and when any deviation is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified. When the end user meets the compliance and informs BEC Campus LAN in writing/by email, connection will be restored.

2.8 For all the computers that were purchased by the BEC centrally and distributed by the BEC Store, BEC Campus LAN will attend the complaints related to any maintenance related problems.

3. Software Installation and Licensing

This section presents BEC software installation and licensing policy. Any computer purchases made by the individual departments/projects 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, BEC IT policy does not allow any pirated/unauthorized software installation on the BEC owned computers and the computers connected to the BEC campus network. In case of any such instances, BEC will hold the department/section/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

3.1 Operating System

3.1.1 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. Checking for updates and updating of the OS should be performed peridically.

3.1.2 BEC encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

3.2 Antivirus Software

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

3.2.2 Individual users should make sure that the software is running correctly. If the end users face any technical difficulty in installation and updating, they may seek assistance from BEC Campus LAN.

3.3 Backups of Data

3.3.1 Individual users should perform regular backups of their vital data. Without proper backups, recovery of destroyed files may be difficult. Preferably, at the time of OS installation itself, one can have the computer’s hard disk partitioned into two volumes. OS and other software should be on one drive and user’s data files on the other drive. In case of any problem, generally only the volume containing OS and other software gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a foolproof solution. Apart from this, users should keep their valuable data in CD/pen drives/hard discs.

4. Network (Intranet & Internet) Usage

Network connectivity provided through the BEC, referred to hereafter as "Network". BEC Campus LAN is responsible for the ongoing maintenance and support of the Network.

4.1 IP Address Allocation

4.1.1 Any computer (PC/Server) that will be connected to the BECnetwork should have an IP address assigned by the BEC Campus LAN DHCP server. Following a systematic approach, the range of IP addresses that will be allocated to each building is decided.

4.2 Running Network Services on the Servers

4.2.1 Individual departments/individuals connecting to the BEC network over the LAN may run server software only after bringing it to the knowledge of the BEC Campus LAN in writing and after meeting the requirements of the BEC IT policy for running such services. Non-compliance with this policy is a direct violation of the BEC IT policy, and will result in termination of their connection to the Network.

4.2.2 BEC Campus LAN will be constrained to disconnect client machines where potentially damaging software is found to exist.

4.2.3 A client machine may also be disconnected if the client's activity adversely affects the Network's performance.

4.2.4 Access to remote networks using a BEC network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the BEC Network connects.

4.2.5 BEC network and computer resources are not to be used for personal commercial purposes.

4.2.6 Network traffic will be monitored for security and for performance reasons at BEC Campus LAN. 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.

4.3 Wireless Local Area Networks

4.3.1 Wireless Local Area Network (WLAN) access must be restricted either via authentication or MAC/IP address restrictions.

4.4 Internet Bandwidth obtained by Other Departments

4.4.1 Internet bandwidth acquired by any section, department of the university under any research programme/project should ideally be pooled with the BEC Internet bandwidth, and be treated as BEC common resource. Under particular circumstances, which prevent any such pooling with the BEC Internet bandwidth, such network should be totally separated from the BEC campus network. All the computer systems using that network should have separate IP address scheme (private as well as public) and the BEC gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the BEC IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to BEC Campus LAN. Non-compliance to this policy will be direct violation of the BEC IT security policy.

5. Web Pages Hosting in Website

5.1 Official Pages

5.1.1 Sections, departments, Employees and Students may have pages on BEC website http://www.becbgk.edu. Official Web pages must conform to the BEC Website Creation Guidelines for Web site hosting. BEC Campus LAN is responsible for maintaining the official web site viz., http://www.becbgk.edu only.

5.2 Personal Pages

5.2.1 Faculty may have their personal pages in official website of the BEC by sending a written request to BEC Campus LAN forwarded through department headalong with the softcopy of the data. 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.

5.3 Web Pages for eLearning

5.3.1 BEC does not have this facility as on this date, this Policy relates to future requirements for Web pages for eLearning authored as a result of Teaching/Learning process. Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the Web, linked through the appropriate department's pages.

5.4 Student Web Pages

5.4.1 BEC does not have this facility as on this date, this policy relates to future requirements for personal student Web pages. Policies for student pages authored as a result of academic assignments. Only web pages of students related to their assignments will be accepted on the Students web pages. The contents of personal pages hosted by the students 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.

6. Email Account

In an effort to increase the efficient distribution of information to all faculty, staff and students, and the BEC administrators, it is planned to set up BEC own domain e-mail services, for formal communication and for academic & other official purposes. BEC does not have this facility as on this date. E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal BEC communications are official notices to faculty, staff and students.

7. Database Usage

This Policy relates to the databases maintained by the BEC Campus LAN. 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. BEC has its own policies regarding the creation of database and access to information and a more generic policy on data access.

7.1 BEC is the data owner of all the institutional data generated in the campus.

7.2 Individual Sections or departments generate portions of data that constitute BEC database. They may have custodianship responsibilities for portions of that data.

7.3 BEC data policy does not allow the distribution of data that is identifiable to an outside person.

7.4 Data from the BEC Database including data collected by departments or individual faculty and staff, is for internal purposes only.

7.5 Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies. All such requests are to be forwarded to the Principal Office

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

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

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

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

7.10 Trying to break security of the Database servers.

Such data tampering actions will result in disciplinary action against the offender by the BEC authorities. If the matter involves illegal action, law enforcement agencies may become involved.

8. Video Surveillance

The system comprises of fixed position IP cameras, NVR, and SAN/NAS Storage and maintained by BEC Campus LAN.

8.1 Cameras are located at strategic points on the campus, principally at the entrance and exit point of sites and buildings.

8.2 No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

8.3 Cameras areusually placed at entrance and exit points of the campus to monitor staff, students, visitors and members of the public.

8.4 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.

8.5 The system has been installed by BEC with the primary purpose of reducing the threat of crime generally, protecting BEC premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy.

8.6 The system will not be used: to provide recorded images for the world-wide-web, for any automated decision taking, and covert recording.

8.7 Staff, students and visitors may be granted access to the system on a case-by-case basis and only then on written authorization from the Principal.

8.8 All staff working in the BEC Campus LAN will be made aware of the sensitivity of handling CCTV/IP Cemera images and recordings. The Coordinator, BEC Campus LANwill ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Cemera.

8.9 Recording will be normally retained for fifteen days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

8.10 All hard drives and recorders shall remain the property of BEC until disposal and destruction.