INFORMATION TECHNOLOGY
POLICY

EAST WEST

INFORMATION TECHNOLOGY (IT) POLICY

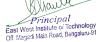# INFORMATION TECHNOLOGY (IT) POLICY

1. Policy statement:

- East West Institute of Technology views Information Technology (IT) as the medium for ensuring optimum dissemination of knowledge through EWIT-ITS

- EWIT 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. Objectives

- IT policy exists to create, maintain, secure, and ensure legal and appropriate use of Information Technology infrastructure established in the 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 institution. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

- EWIT aims at identifying, providing and maintaining reliable computing facilities, computing network environment, communication facilities and related infrastructure to facilitate education and research.

Note:

- In this document, the term "users" shall mean individuals, staff, students, faculty, departments, offices or any other entity which fall under the management of EWIT campus and require any services aforesaid. 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.

- The term "ITS" shall mean EWIT IT Services.

3. **Acceptable IT Devices:**

   Any computer, peripheral or network capable device connected to campus network must belong to, or be formally registered, or be hosted by, Shall reserve the rights to restrict the access of the IT Systems.

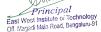4. **Responsibilities of Users and User groups:**

   - Following copyright laws regarding protected commercial software or intellectual property.

   - Honoring acceptable computer use policy of computer networks accessed through EWIT campus network either locally or remotely.

   - 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.

5. ## Data network responsibilities of end users

   - Individual department, users or user groups may develop their own local area networks or local communications environment within, only if those facilities are approved by and meets developed network standards. EWIT-ITS shall also reserve the rights to monitor such networks.

   - Any user group or department intending to establish connectivity to external data communications network directly should do so after coordinating with EWIT-ITS. EWIT-ITS 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 center of EWIT-ITS to maintain security to the campus network.

6. ## Computing facility provisioning and maintenance.

   - EWIT-ITS is responsible for provision and maintenance of computing facilities provided to users. The facilities are provided after the user secure approvals from the management.

   - The user shall ensure physical safety of the equipment and produce the same as and when required for stock verification by EWIT-ITS. If any peripheral or components of the equipment assigned is found missing, the user shall report the same to EWIT-ITS for further action. The user shall obtain prior approval from EWIT-ITS before plugging in any additional peripherals to the

---

local area network (LAN). This is also applicable to connect peripherals to external ports like USB, RS232 etc. EWIT-ITS shall not be responsible for any failure to personal peripherals connected to institute equipment by the user. Users shall ensure data availability and security by taking regular backups of the data stored on their systems.

- The individual or the department shall be responsible to report any hardware or software related faults to EWIT-ITS through facilities provided for reporting. EWIT-ITS shall take all necessary steps to resolve the issue at the earliest. However, faults that require substantial additional financial expense may need to be approved by competent authorities.

- The ownership of the equipment assigned to the individual or the department shall remain with EWIT.

7. Provision of computing software and maintenance

- EWIT-ITS shall provide all necessary software for operating the devices allocated to the user.

- EWIT-ITS reserves the right to secure the **administrative passwords** for all the devices owned by the Institute.

- Users may install any software on the equipment allotted to them after obtaining prior approval from concerned department head. All such software that may be installed on the equipment shall be used for official purposes. However, EWIT-ITS 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.

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

8. Provisions of Network Connectivity and Maintenance

- EWIT-ITS is responsible for providing users with data communications connectivity from their building to all campus-wide network services.

Principal
East West Institute of Technology
Off. Magadi Main Road, Bengaluru-91

- EWIT-ITS 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.

9. LAN Security

- EWIT-ITS 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.

- EWIT-ITS is responsible for the integrity of all software running on the backbone network equipment, including servers, LAN switches, routers, and gateways.

- Users are encouraged to assist EWIT-ITS 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.

- EWIT-ITS 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.

- EWIT-ITS shall also extend support to users connecting their personal devices to the campus network but limited to the operational or legal constraints.

10. Provision of network services:

i. EWIT-ITS shall host all necessary network services to support the activities of the users. This shall include internet connectivity, email services, DNS etc. The usage of the services shall be for the official purpose. These services are provided for the purpose of increasing the job fulfillment, job performance, and to increase the productivity.

ii. 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 to ensure access security.

iii. Users shall not use EWIT network services to view, download, save, receive, or send material related to or including:

    a) Offensive content of any kind, including pornographic material

    b) Promoting discrimination based on race, gender, national origin, age, marital status, sexual Orientation, religion or disability.

    c) Threatening or violent behavior.

    d) Illegal activities.

    e) Commercial messages.

    f) Messages of a political or racial nature.

    g) Gambling.

    h) Personal financial gain.

    i) Forwarding e-mail chain letters.

    j) Spamming e-mail accounts from e-mail services or computers.

    k) Material protected under copyright laws.

    l) Sending business-sensitive information by e-mail or over the Internet.

    m) Dispersing organizational data to personnel without authorization.

    n) Opening files received from the Internet without performing a virus scan.

    o) Recreational streaming of internet material, such as radio, video, TV, or stock tickers

    p) Downloading and/or installing programs/software on any network computer(s) without authorization from the ITMS.

iv. ITMS may shutdown the network services periodically for maintenance purposes. Users shall

be informed well in advance regarding such outages.

v.   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.

11. Network activities not permitted over the campus network

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

- Activities that violate rules of local administration, the State, Central Government or recognized International Organization or Treaties.

- 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.)

- Configuring mail servers with open relays, sending unsolicited mails, commercial mails, spamming. Downloading large files for personal use including music, video and software.

- Probing, scanning or other activities that amount enumeration of campus network.

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

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

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

- Illegal distribution of any copyrighted material.

- "Stealing" or "Borrowing" IP addresses.

  Any activity that tarnishes EWIT's professional image.

IT-Policy   Page 6

12. Violations

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

- If it is confirmed and proved 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.

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

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

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

****

Principal
East West Institute of Technology
Off. Magadi Main Road, Bengaluru-91

Subramanya Education Society

EAST WEST INSTITUTE OF TECHNOLOGY

No. 63, East West College Road, Off, Magadi Main Rd, Vishwaneedam Post, Bharath Nagar, Anjana Nagar, Bengaluru, Karnataka 560091   **www.ewit.edu.in**

Principal
East West Institute of Technology
Off. Magadi Main Road, Bengaluru-91