ICT POLICY

PREFACE

Fairfield Institute of Management and Technology (FIMT) is committed to promoting a culture of seamless communication, collaboration, and knowledge sharing through the purposeful adoption of Information and Communication Technology (ICT). Aligned with the UGC Guidelines for the Institutional Development Plan for Higher Education Institutions and the vision of a 'Digital India' articulated in the NEP 2020, the institute strives to move towards a fully integrated digital ecosystem.

To support this vision and acknowledging the growing dependence on technology for academic and administrative functions, FIMT adopts this comprehensive ICT Policy. The policy aims to ensure that all ICT resources are utilized in a secure, efficient, and responsible manner. It seeks to minimize risks and institutional liabilities, enhance operational effectiveness, safeguard digital assets, and uphold the integrity and security of institutional data.

OBJECTIVES

This policy therefore aims outlining the regulations and guidelines for the proper use of the ICT resources and systems made available to the users by or on behalf of the institution including desktops, laptops, mobile phones, network devices, internet, intranet, Wi-Fi, external storage devices, and peripherals like printers, scanners, copying machines, and such other equipment. It also applies to use of world-wide-web, blogs and wikis, e-mails, social networking or collaboration services.

The objectives of this policy are:

1. To regulate ICT Resource Usage

Establish regulations and guidelines for the proper use of ICT resources and systems made available by the Institution.

2. To ensure Secure and Responsible Use

Promote secure and responsible use of ICT resources, including desktops, laptops, mobile phones,

network devices, internet, intranet, Wi-Fi, and peripherals.

3. To govern Online Activities

Regulate the use of online platforms, including the world-wide-web, blogs, wikis, e-mails, social networking, collaboration services, and system and application software.

4. To protect FIMT'S Assets

Safeguard Institution's ICT assets, services, and databases from unauthorized access, misuse, and other security threats.

ICT POLICY

5. To foster a Culture of Compliance

Educate users about their responsibilities and obligations when using Institution's ICT resources, ensuring a culture of compliance and responsible ICT usage.

SCOPE & APPLICIBALITY

This policy, supplemented by the following policies, applies to all users of the institution's computing, networking, and IT facilities, including students, faculty, staff, and administration.
It is also applicable to the third-party contractors, agents, and suppliers wherever they are involved.

1. Hardware Procurement and Maintenance Policy
2. System Condemnation Policy
3. Website Policy
4. E-Mail Usage Policy
5. Anti-Virus Policy
6. Usage Policy
7. Network Access Monitoring Policy
8. Server Access and Maintenance Policy

GENERAL POLICIES

These policies collectively govern the use of IT resources and ensure their secure, efficient, and effective operation.

- Services and applications that will not be used must be disabled where possible.
- Access to services should be logged and/or protected through access-control.
- The most recent security patches must be installed on the system as soon as practical.
- Trust relationships between systems are a security risk, and their use should be avoided.
- Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas

ICT POLICY

MONITORING

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs would be kept online for a minimum of 1 year.
- Daily incremental backups will be retained for at least 1 week.
- Weekly full backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 3 years.

ROUTINE PRECAUTIONS

- Only authorized administrators are authorized to login to the mail, web, proxy and other servers.
- The designated system administrator/operational group receives an email alert whenever such an advice is released by the official maintainers of the software.
- The software is updated periodically and whenever required.
- All ports except those necessary for functioning of the servers are blocked (firewalled) both from outside and inside.
- Standard intrusion detection software is run on the FIMT network to monitor any change of MAC addresses corresponding to IP addresses of trusted machines. The Systems Manager automatically receives an email alert in such cases.