Policy for Fair Usage of Information Systems

1. Policy Brief & Purpose

Authorized users may access the institute's information assets for educational, academic, research, and administrative purposes. Users must follow safe, ethical, and appropriate usage practices that do not interfere with institute operations, compromise information security, or damage the institute's reputation.

2. Scope

This policy applies to all personnel assigned or granted access to institute-owned or institute-managed devices, systems, applications, networks, or internet services, including faculty, staff, students, researchers, contractors, consultants, interns, and external partners.

3. Policy Elements and Responsibilities

Users are responsible for maintaining the security of laptops, desktops, mobile devices, and other systems used to access institute resources. Appropriate measures shall be taken to prevent unauthorized logical or physical access.

Users bear full responsibility for all actions performed using their LDAP, MIS, email, VPN, or any other institutional credentials. Users must maintain the confidentiality of their credentials, use strong passwords, and must not share credentials with any third party.

Users must promptly report suspected security incidents, phishing attempts, malware infections, unauthorized access, or data breaches to the designated IT or Information Security team.

4. Inappropriate Use of Institute Assets

The following activities are prohibited unless explicitly authorized by the institute:

a. Unauthorized vulnerability scanning, penetration testing, traffic generation, or security testing against internal or external systems.

b. Downloading, distributing, storing, or sharing copyrighted material or software in violation of applicable laws or license agreements.

c. Installing, using, copying, or distributing pirated, cracked, or unlicensed software or media, including attempts to bypass license enforcement or copy-protection mechanisms.

d. Disrupting or interfering with computers, networks, users, services, or equipment, including intentional disruption of systems, applications, or network operations.

e. Using institute IT infrastructure for unauthorized commercial activities or for hosting services, applications, or data on behalf of external individuals or organizations.

f. Accessing, storing, transmitting, or distributing content that is unlawful, harassing, discriminatory, defamatory, obscene, or otherwise inconsistent with institute policies.

g. Using anonymization, tunneling, proxy, or similar services intended to bypass institutional monitoring, network controls, or security mechanisms without authorization.

5. Measures for Securing Information Assets

Users shall:

a. Enable device security controls such as BIOS/UEFI passwords, screen locks, and disk encryption, where appropriate.

b. Lock devices when unattended and shut down systems when appropriate.

c. Ensure that operating systems, firmware, applications, browsers, endpoint protection software, and video-conferencing applications are updated with the latest supported security patches and updates.

d. Ensure that antivirus or endpoint protection solutions are installed and updated with the latest definitions and security signatures.

e. Use only appropriately licensed software, including institute-approved, academic-licensed, or open-source software where feasible.

f. Avoid installing unnecessary browser extensions, plugins, toolbars, or software from untrusted sources.

g. Exercise caution when opening shortened URLs, email attachments, QR codes, or links from untrusted or unsolicited sources, as these may lead to phishing or malware attacks.

h. Protect institutional data from unauthorized disclosure, modification, destruction, or sharing.

6. Exceptions

Requests for exemptions from captive portal requirements or related network access controls must be formally approved by the competent authority designated by the institute. The Dean (Infrastructure) shall serve as the approving authority for such exceptions. Approved users remain responsible for ensuring that such access does not compromise institutional security, monitoring, compliance, or operational requirements.

7. Monitoring and Compliance

The institute reserves the right to monitor, log, audit, and review the usage of institutional information systems and networks to ensure security, compliance, operational continuity, and enforcement of institute policies, subject to applicable laws and regulations.

All users must comply with applicable laws, Government of India regulations, and guidelines issued by CERT-In, NIC, or other authorized governmental agencies.

8. Violations and Enforcement

Violation of this policy may result in suspension or revocation of access privileges, disciplinary action, financial liability, and/or legal proceedings in accordance with institute regulations and applicable laws.

9. Policy Review

This policy shall be reviewed periodically and updated as necessary to address changes in technology, security requirements, legal obligations, and institutional needs.