NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA
ODISHA, 769008, INDIA

Computer Assets and IT Infrastructure Usage Policy

1. Purpose

The purpose of this IT Infrastructure Usage Policy is to establish guidelines and procedures to protect the Institute's information assets, digital infrastructure, and technology resources from unauthorized access, misuse, damage, or loss.

The policy aims to:

- Safeguard the confidentiality, integrity, reliability and availability of sensitive institutional, research, and personal data.
- Protect the IT assets and services of the Institution against unauthorised access, intrusion, disruption or other damages.
- Prevent cyber threats such as hacking, malware, phishing, and data breaches and create a secure IT ecosystem to provide academic and research freedom within secure boundaries.
- Promote responsible and ethical use of IT resources.
- Ensure compliance with national cybersecurity laws (e.g., IT Act 2000 and its amendments, CERT-In guidelines).
- Establish accountability and incident response mechanisms.

2. Applicability

This policy applies to:

- All faculty, staff, students, researchers, contractors, vendors, and visitors using the Institute's IT resources.
- All Institute-owned or managed IT assets including servers, storage, networks, workstations, cloud services, research databases, and communication systems.

3. Policy Statement

IT/ICT resources provided by the institute should only be used for the purpose of teaching, learning and research by the users. It is the responsibility of the users to appropriately use and protect institutional IT resources and to respect the rights of others.

This policy is a guideline for safer and legitimate use of such IT resources and infrastructure available in the Institution.

4. IT Governance

- Server Administrators, Network Administrators and Desktop Support Team will be responsible deployment, monitoring, incident response and enforcement of the policies.
- The **Institute IT Security Committee (ITSC)** shall oversee the implementation and enforcement of these policies.
- The **Chief Information Security Officer (CISO)** and **Deputy CISO** will coordinate all cybersecurity initiatives, ensure compliance, assist onboarding / off-boarding and escalate issues.

5. Acceptable Use Policy

All users of the Institute's IT resources must adhere to the following guidelines to ensure secure, ethical, and responsible use of technology and information systems.

5.1 Authorized and Appropriate Use

Users must:

- Use IT resources exclusively for academic, research, administrative, and officially approved purposes.
- Access web services, e-resources, intranet, email, and computational facilities only through authorized login and authentication procedures.
- Avoid using institutional IT resources for personal business, unauthorized activities, or commercial profit.

5.2 Account and Authentication Security

Users must:

- Protect account credentials and **must not share** passwords, access tokens, or OTPs with anyone.
- Use **multi-factor authentication (MFA)** for email, administrative accounts, and other critical systems.
- Change passwords regularly and use strong, complex passwords that cannot be easily guessed.

5.3 Safe Browsing and Email Practices

Users must:

- Avoid clicking on suspicious links or opening unknown email attachments; all attachments should be scanned before opening.
- Not access illegal websites, pirated content platforms, or any site that violates laws or Institute policy.
- Refrain from downloading or installing unlicensed, pirated, or unauthorized software.

5.4 Content Restrictions

Users must not:

- Send, view, upload, download, or display content that is offensive, obscene, pornographic, fraudulent, threatening, harassing, or otherwise prohibited by law or policy.
- Host, distribute, or share illegal, pirated, defamatory, or harmful materials through any Institute IT resources or social media platforms.
- Contribute to a hostile academic or work environment through inappropriate digital conduct.

5.5 Network and Infrastructure Security

Users must:

- Not tamper with or physically alter any network cables, ports, or equipment.
- Not install unauthorized hardware such as Wi-Fi access points, routers, or switches; only approved and registered devices may connect to the official network.
- Not attempt to bypass network security using unauthorized VPNs, proxies, tunnelling tools, or anonymizers.
- Not attempt to access, penetrate, scan, or interfere with servers, databases, storage systems, surveillance equipment, or any restricted system without proper authorization.

5.6 System, Device, and Software Security

Users must:

- Keep all operating systems, applications, and software updated regularly with official patches.
- Install and maintain Institute-approved **Antivirus or Endpoint Detection and Response (EDR)** software on all devices.
- Perform periodic scans for viruses, malware, bots, and other security threats.
- Enable firewalls on all endpoints and ensure they remain active at all times.

- Not use unknown, unverified, or unauthorized USB/external drives or media devices.

5.7 Data Protection and Privacy

Users must:

- Respect the privacy of others and must not attempt to access any personal device or data without explicit permission.
- Encrypt sensitive or confidential data during storage and transmission.
- Not share, disclose, or disseminate confidential or official information without proper authorization.
- Securely delete Institute data when it is no longer required and ensure that sensitive information is not recoverable.
- Not vandalize, manipulate, or modify data, whether intentionally or accidentally.

5.8 Backups of Data

Users must:

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

5.9 Responsible Use of Shared Resources

Users must:

- Use bandwidth, network access, and shared computing resources responsibly, avoiding excessive or wasteful usage that may impact others.
- Ensure that resource-heavy activities are approved and scheduled appropriately.

5.10 Reporting Duties

Users must:

- Immediately report any suspicious activities, security incidents, or anomalies such as phishing attempts, malware infections, unauthorized access, or lost/stolen devices.
- Notify the IT team promptly if any system or account compromise is suspected.

6. Prohibited Usage

The users shall not send, view or download fraudulent, harassing, obscene, threatening, or other messages or material that are a violation of applicable law or Institute policy. In particular, contributing to the creation of a hostile academic or work environment is prohibited.

7. Social Media Usage

Users must ensure responsible and ethical use of all social media and online communication platforms. This includes social networking sites, mailing lists, forums, news groups, chat rooms, blogs, and collaborative online tools. Users are expected to:

- Follow all Institute policies, guidelines, and codes of conduct when posting, commenting, sharing, or engaging on any online platform.
- Ensure that no confidential, sensitive, or proprietary Institute information is disclosed through social media.
- Avoid posting content that could harm the reputation of the Institute, its members, or its stakeholders.
- Refrain from sharing offensive, defamatory, inflammatory, or misleading information on any online platform.
- Use social media and online communication tools in a manner that does not disrupt Institute operations or violate legal, ethical, and institutional standards.

8. Commercial Use

The Institute IT resources shall not be used for any commercial and promotional purposes, through advertisements, solicitations or any other message passing medium, except as permitted under Institute rules and other uses approved by the competent authority.

9. Copyrights and Licenses

Users must strictly adhere to all applicable copyright laws, intellectual property rights, and software licensing agreements when accessing, using, or sharing digital content through the Institute's IT resources. This includes academic materials, software, media files, publications, datasets, and any other protected content.

Users must:

- Use copyrighted materials only in accordance with permitted academic, research, or licensed usage.
- Refrain from copying, distributing, downloading, uploading, or sharing copyrighted content without proper authorization or valid licenses.
- Ensure that all software installed on Institute-owned or personal devices used for Institute work is properly licensed and legally obtained.
- Avoid the use of pirated, cracked, or unauthorized software under any circumstances.
- Understand that **unlawful file-sharing**, including peer-to-peer sharing of protected content (such as movies, music, software, or publications) using Institute networks, is strictly prohibited and constitutes a violation of this policy and legal provisions.

Any violation of copyright or licensing rules may lead to disciplinary action and legal consequences under applicable intellectual property laws.

10. Monitoring and Regulation

The IT resources used by the user are subject to monitoring and regulation. The Institute reserves its right to perform necessary actions to protect and to preserve the overall integrity and efficiency of the Institute network.

11. Disabling IT Resource/ User's Network Connectivity

The Institute holds responsibility of managing and protecting the NIT Rourkela network(s) against electronic forms of attack or abuse. It is the sole prerogative of the Institute to terminate network connections to an offending computer(s) within its domain due to suspected or actual abuse of the network and/or its components.

12. Teamwork and Cooperation

The Institute solicits wholehearted cooperation and sincere support from its users of IT resource during any investigation of policy abuse and/ or cybercrime. Instances of non-cooperation from any user shall constitute the grounds for suspension or cancellation of access to IT resources or other disciplinary actions.

13. Non-compliance of CAIT Policy and Consequent Abuse

Non-compliance of this Policy and consequent abuse of IT resources may attract appropriate disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action. Violation of this policy may also indicate that a user may also have violated the legal prerogatives as permitted under prevailing cyber laws and acts. If established, such action may also lead to severe civil or criminal proceedings as per the

applicable laws and provisions. The Chief Information Security Officer (CISO) will refer such violations to the Director, NIT Rourkela for seeking further necessary directions.

CAUTION: Various laws as applicable in real world may also be applicable in cyberspace (including NIT Rourkela's IT infrastructure). Users of IT resources are not exempted from existing laws about libel, harassment, privacy, copyright, licenses, stealing, threats, etc. Taking precautions and preventive measures while using cyber space and IT resources may be the best saviour. Any abuse of IT resources may lead to severe consequences and legal proceedings.
