TATA STEEL SPECIAL ECONOMIC ZONE

Prohibited Activities under IT Act 2000

(Revision 01.00)

Date – 01/07/2026

Purpose

This policy establishes the standards of acceptable use of the organization's information and communication systems and prohibits activities that violate the Information Technology Act, 2000, and other applicable laws of India. It applies to all employees, contractors, consultants, vendors, and third parties who access or use the organization's IT resources.

Scope

This policy covers all computers, servers, networks, mobile devices, cloud services, email systems, applications, databases, internet access, and digital communication platforms owned, managed, or used by the organization.

Prohibited Activities

The following activities are strictly prohibited:

1. **Unauthorized Access**
    - Accessing systems, applications, databases, or information without authorization.
    - Attempting to bypass security controls or authentication mechanisms.
2. **Data Theft or Misuse**
    - Copying, downloading, deleting, altering, or transmitting confidential or proprietary information without authorization.
    - Unauthorized sharing of company, customer, or employee data.
3. **Identity Theft and Impersonation**
    - Using another person's credentials, password, or digital identity.
    - Creating fake identities or impersonating individuals through electronic means.
4. **Cyber Fraud**
    - Engaging in phishing, spoofing, online fraud, or deceptive electronic communications.
    - Manipulating electronic records for financial or personal gain.

5. **Malware and System Damage**
    - Introducing viruses, ransomware, spyware, malicious code, or any software intended to damage or disrupt systems.
    - Attempting to interfere with network availability or business operations.
6. **Privacy Violations**
    - Unauthorized monitoring, recording, interception, or disclosure of electronic communications.
    - Accessing personal or confidential information without legitimate business authorization.
7. **Publication or Transmission of Illegal Content**
    - Creating, storing, transmitting, or distributing obscene, sexually explicit, defamatory, hateful, or otherwise unlawful content.
    - Sharing content prohibited under applicable Indian laws.
8. **Intellectual Property Violations**
    - Unauthorized copying or distribution of copyrighted software, documents, media, or other intellectual property.
    - Use of unlicensed software.
9. **Tampering with Electronic Records**
    - Altering, destroying, or concealing electronic records, logs, or evidence.
    - Modifying source code or system files without authorization.
10. **Misuse of Organizational IT Resources**
    - Using company IT resources for illegal, unethical, or unauthorized commercial activities.
    - Operating unauthorized software, services, or devices on the organizational network.

Employee Responsibilities

Employees shall:

- Use IT resources responsibly and only for authorized business purposes.
- Protect passwords and authentication credentials.
- Immediately report any suspected cybersecurity incident or policy violation.
- Cooperate with investigations relating to cybersecurity incidents.

Monitoring

The organization reserves the right to monitor, log, audit, and review the use of its IT resources in accordance with applicable laws and organizational policies.

Violations

Violation of this policy may result in:

- Disciplinary action up to and including termination of employment or contract.
- Recovery of damages where applicable.
- Civil and criminal proceedings under applicable laws, including the Information Technology Act, 2000.

Relevant Provisions of the Information Technology Act

The policy aligns with key provisions of the Information Technology Act, 2000, including:

- Section 43 – Unauthorized access and damage to computer systems
- Section 65 – Tampering with computer source documents
- Section 66 – Computer-related offences
- Section 66B – Receiving stolen computer resources
- Section 66C – Identity theft
- Section 66D – Cheating by personation using computer resources
- Section 66E – Violation of privacy
- Section 66F – Cyber terrorism
- Sections 67, 67A, and 67B – Publication or transmission of obscene, sexually explicit, and child sexual abuse material in electronic form

Review

This policy shall be reviewed periodically or whenever there are significant changes in applicable laws, technology, or organizational requirements.

Note: This policy supersedes all the communication on the subject till date. In case of any deviation from the existing policy, the MD will have the authority to approve on a case-to-case basis in the interest of the business.

Approved by

Manikanta Naik

Managing Director