भारतीय पटसन निगम लिमिटेड

The Jute Corporation of India Limited

(A Government of India Enterprise)

प्रधान कार्यालय: पटसन भवन, तीसरी और चौथी मंजिल, ब्लॉक-सीएफ, एक्शन एरिया - 1, न्यू टाउन, कोलकाता - **700156**

Head Office: Patsan Bhavan, 3rd & 4th Floor, Block-CF, Action Area – 1, New Town, Kolkata - 700156

संदर्भ सं.:भापनि/सू.प्रौ./नीति/2025-26/01 दिनांक : 02.06.2025

प रि प त्र

उपयुक्त प्राधिकारियों द्वारा अनुमोदित एन्क्रिप्टेड स्टोरेज और ट्रांसमिशन नीति एवं आईटी परिसंपति निपटान नीति इसके साथ परिचालित किया जा रहा है।

निगम के सभी कर्मचारियों द्वारा इसका सख्ती से अनुपालन करना है।

इसका सक्षम प्राधिकारी का अनुमोदन प्राप्त है।

शन्तनू चक्रवर्ती

(शन्तनू चक्रवर्ती)
विभागाध्यक्ष(सू.प्रौ.)

अनुलग्नक:

1. एन्क्रिप्टेड स्टोरेज और ट्रांसमिशन नीति v1.0
2. आईटी परिसंपति निपटान नीति v1.0

परिचालन:

1. प्रबंध निदेशक के सचिवालय - प्रबंध निदेशक महोदय को सूचनार्थ।
2. निदेशक(वित्त) के सचिवालय - निदेशक(वित्त) महोदय को सूचनार्थ।
3. मुख्य सर्तकता अधिकारी
4. मुख्य सूचना सुरक्षा अधिकारी
5. महाप्रबंधक(परि./विप.)/उप महाप्रबंधक(वित्त)
6. मुख्य प्रबंधकगण/वरिष्ठ प्रबंधकगण/प्रबंधकगण
7. क्षेत्रीय प्रबंधकगण/उप प्रबंधकगण/सहायक प्रबंधकगण/सू.प्रौ.अधिकारी/मा.सं.अधिकारीगण
8. क्षे.का./आरएलडी - इस अनुरोध के साथ कि वे इसे क्षेत्र के कर्मचारियों के बीच परिचालित करें।
9. निगम के सभी कर्मचारीगण
10. वेबसाइट

भारतीय पटसन निगम लिमिटेड
(भारत सरकार का उपक्रम)
The Jute Corporation of India Limited
(A Government of India Enterprise)
पंजीकृत और प्रधान कार्यालय: पटसन भवन, तीसरी और चौथी मंजिल,सी एफ ब्लॉक, एक्शन एरिया I ,
न्यू टाउन, पश्चिम बंगाल - 700156
Head Office: Patsan Bhavan, 3rd & 4th Floor, CF Block, Action Area I ,
New Town, West Bengal - 700156
सी.आई.एन./ C.I.N.: U17232WB1971GOI027958

Ref No.: JCI/IT/Policy/2025-26/01 Date: 02/06/2025

Circular

Encrypted Storage and Transmission Policy and IT Asset Disposal Policy as approved by the Appropriate Authorities are being circulated herewith.

The same are to be strictly adhered to and complied with, by all employees of the Corporation.

This has the approval of competent authority.

(Santanu Chakraborty)
Head of the Department (IT)

Enclosures:

1. Encrypted Storage and Transmission Policy v1.0
2. IT Asset Disposal Policy v1.0

Circulation:

1. MD's Secretariat – for information of MD
2. D(F)'s Secretariat – for information of D(F)
3. CVO
4. CISO
5. GM(O/M) / DGM (F)
6. Chief Managers / Senior Managers / Managers
7. Regional Managers / Deputy Managers / Assistant Managers / IT Officer / HR Officers
8. RO / RLD – with a request to circulate among employees of the Region
9. All Employees of the Corporation
10. Website

Encrypted Storage and Transmission Policy

Version 1.0

THE JUTE CORPORATION OF INDIA LIMITED (JCI)
PATSAN BHAWAN
ACTION AREA – 1, CF BLOCK
NEW TOWN
KOLKATA-700156

EFFECTIVE DATE: 01/06/2025
PLACE: KOLKATA

1 CONTENTS

2 INTRODUCTION

In today's digital landscape, data is a critical asset for The Jute Corporation of India Limited (JCI). This data, whether it be customer information, financial records, or intellectual property, must be protected from unauthorized access, disclosure, or theft. Encryption is a fundamental security measure that plays a vital role in achieving this protection.

Encryption is the process of converting information into an unreadable format, known as "ciphertext," so that it cannot be understood by anyone without the proper decryption key. This policy outlines JCI's requirements for encrypting sensitive data, both when it is stored (at rest) and when it is being transmitted across networks (in transit).

The purpose of this policy is to establish a framework that ensures the confidentiality, integrity, and availability of JCI's sensitive information. By adhering to the guidelines set forth in this policy, JCI aims to:

- Minimize the risk of data breaches and unauthorized access.
- Protect the privacy of individuals whose data we handle.
- Maintain the trust of our customers, partners, and stakeholders.
- Comply with relevant legal and regulatory requirements.

This policy applies to all employees, contractors, and authorized users who access, use, or manage JCI's data. It is essential that all personnel understand and comply with the requirements outlined in this document to safeguard JCI's valuable information assets.

3 PURPOSE

To safeguard JCI’s sensitive and valuable information from unauthorized access or theft, especially when stored or transmitted over public and private networks accessed by JCI.

4 SCOPE

This Encrypted Storage and Transmission Policy applies to all sensitive data owned, accessed, stored, or transmitted by The Jute Corporation of India Limited (JCI), its employees, contractors, and authorized users. This includes, but is not limited to, the following categories of data, regardless of the storage medium or transmission method:

- **Personal Information:** Any information relating to an identified or identifiable natural person, such as:

  - Employee records (e.g., names, addresses, social security numbers, contact information, payroll data, performance reviews).
  - Customer data (e.g., names, contact information, transaction history).
  - Supplier and vendor information.
  - Jute seller data / information.
- **Confidential Business Data:** Information that is not publicly available and is critical to JCI's operations, including:
  - Financial records (e.g., budgets, financial statements, forecasts).
  - Strategic plans and business development information.
  - Marketing plans and sales data.
  - Legal documents and correspondence.
- **Proprietary Intellectual Property:** Information that gives JCI a competitive advantage, such as:
  - Trade secrets.
  - Inventions and patents.
  - Technical specifications and designs.
  - Proprietary software code.
- **Other Sensitive Data**: Any other data that is classified as confidential, sensitive, or critical to JCI's operations, reputation, or legal obligations.

This policy applies to all systems and devices used to store, process, or transmit JCI's Aadhaar related data, including but not limited to:

- Desktop computers and laptops used for Aadhaar authentication in the Corporation.
- Mobile devices (e.g., smartphones, tablets) used for Aadhaar authentication in the Corporation.
- Servers and network infrastructure used for Aadhaar authentication in the Corporation.
- Cloud storage and applications used for Aadhaar authentication in the Corporation.
- Removable media (e.g., USB drives, external hard drives) used for Aadhaar authentication in the Corporation.
- Communication systems (e.g., email, instant messaging) used for Aadhaar authentication in the Corporation.
- Internet of Things (IoT) devices used for Aadhaar authentication in the Corporation.

- Any other device or system that processes Aadhaar authentication in the Corporation.

The requirements of this policy extend to all forms of data transmission, including but not limited to:

- Electronic mail.
- File transfer protocol (FTP).
- Web browsing.
- Virtual private networks (VPNs).
- Application programming interfaces (APIs).
- Wireless communications.
- Physical transfer of digital media.
- Any other method of data transfer.

5 GLOSSARY

- **Encryption:** The process of converting data into an unreadable format (ciphertext) to prevent unauthorized access. Encryption ensures that only individuals with the correct decryption key can read the information.
- **Decryption:** The reverse process of encryption, where ciphertext is transformed back into its original, readable format (plaintext) using a decryption key.
- **Ciphertext:** The scrambled or encrypted form of data, making it unintelligible to anyone without the decryption key.
- **Plaintext:** Data in its original, readable format, before encryption or after decryption.
- **Key:** A secret piece of information (a string of characters) used by an encryption algorithm to encrypt or decrypt data.
- **Symmetric Encryption:** An encryption method that uses the same key for both encryption and decryption. Examples include AES.
- **Asymmetric Encryption:** An encryption method that uses two keys: a public key for encryption and a private key for decryption. Examples include RSA and ECC.
- **AES (Advanced Encryption Standard):** A symmetric encryption algorithm widely used for securing electronic data. It is a robust and efficient algorithm that is difficult to break.
- **RSA (Rivest–Shamir–Adleman):** A public-key cryptosystem that is widely used for secure data transmission.

- **ECC (Elliptic Curve Cryptography):** A public-key cryptosystem based on the mathematics of elliptic curves.
- **TLS (Transport Layer Security):** A cryptographic protocol used to provide secure communications over computer networks. TLS is commonly used to encrypt web traffic (HTTPS).
- **SSL (Secure Sockets Layer):** An older cryptographic protocol that has been largely superseded by TLS, but the terms are often used interchangeably.
- **Key Management:** The processes and procedures for generating, storing, distributing, and destroying encryption keys. Effective key management is crucial for maintaining the security of encrypted data.
- **Data at Rest:** Data that is stored on a storage device, such as a hard drive, USB drive, or in cloud storage.
- **Data in Transit:** Data that is being transmitted over a network, such as the internet or a local area network.
- **Full Disk Encryption (FDE):** Encrypts all data on a hard drive or other storage device.
- **Hardware Security Module (HSM):** A dedicated hardware device that securely stores and manages encryption keys.
- **Key Management System (KMS):** A system that manages the lifecycle of encryption keys, including generation, storage, distribution, and destruction.
- **BIS:** The Bureau of Indian Standards (BIS) is the national standards body of India, responsible for setting and maintaining standards for various products and services, including those related to information technology and cybersecurity.
- **MeitY**: Stands for the Ministry of Electronics and Information Technology, a government ministry in India responsible for formulating and implementing policies related to electronics, information technology, and related industries.

6 Encryption Methods

JCI employs robust and industry-standard encryption algorithms and techniques to protect the confidentiality and integrity of its sensitive data. The selection of specific encryption methods is based on factors such as the sensitivity of the data, the storage medium, and the transmission channel, and regulatory requirements.

6.1 Encryption Algorithm Standards

- JCI will primarily utilize the Advanced Encryption Standard (AES) with a minimum key length of 256 bits for symmetric encryption. Other BIS or MeitY approved algorithms

may be used where appropriate and after evaluation by the IT Security team and the data owner.

- For asymmetric encryption, JCI will use algorithms such as RSA (Rivest–Shamir–Adleman) or ECC (Elliptic Curve Cryptography), with minimum key lengths as recommended by MeitY guidelines.
- All encryption algorithms and key lengths must adhere to industry best practices and be approved by JCI's IT Security.
- The use of deprecated or weak encryption algorithms is strictly prohibited.

6.2 Data at Rest Encryption

- **Full Disk Encryption:** All laptops, desktops, and other portable devices used to store sensitive data must utilize full disk encryption (e.g., BitLocker, FileVault) to protect data in case of loss or theft.
- **File/Folder Encryption:** For specific files or folders containing sensitive information stored on shared drives or servers, encryption tools (e.g., EFS, VeraCrypt) will be used.
- **Database Encryption:** Databases containing sensitive data will be encrypted at the database level or using Transparent Data Encryption (TDE) where supported by the database management system.
- **Cloud Storage Encryption:** Data stored in cloud environments will be encrypted using encryption mechanisms provided by the cloud service provider, ensuring that JCI maintains control of the encryption keys whenever possible. JCI must approve the provider's encryption methods.
- **Removable Media Encryption:** All removable media (e.g., USB drives, external hard drives) used to store sensitive data must be encrypted.
- **Backup Encryption:** All backups of systems and data containing sensitive information must be encrypted using strong encryption algorithms. The encryption method must be consistent with the sensitivity of the data being backed up.

6.3 Data in Transit Encryption

- **TLS/SSL:** All data transmitted over public or untrusted networks must be encrypted using Transport Layer Security (TLS) protocol, version 1.2 or later. Secure Sockets Layer (SSL) is prohibited.
- **VPNs:** Virtual Private Networks (VPNs) will be used to create secure, encrypted connections for remote access to JCI's network.
- **Email Encryption:** Sensitive information transmitted via email must be encrypted using S/MIME or other approved email encryption methods.
- **Secure File Transfer:** File transfer protocols such as SFTP (Secure FTP) or FTPS (FTP Secure) will be used for transferring sensitive files.

- **Wireless Network Security:** All wireless networks used to transmit sensitive data must be secured using strong encryption (e.g., WPA2/WPA3).
- **Messaging Applications:** Sensitive data transmitted via messaging applications must be end-to-end encrypted.

6.4 Algorithm and Key Strength Updates

- The IT Security team is responsible for monitoring industry best practices and vulnerabilities related to encryption algorithms and key lengths.
- Encryption algorithms and key strengths will be reviewed and updated periodically, at least annually, to ensure they meet current security standards and provide adequate protection against evolving threats.
- Any changes to encryption algorithms or key lengths will be documented, communicated to relevant personnel, and approved by management.
- A process for migrating to new encryption algorithms and key lengths will be established and followed.

7 Key Management

Secure key management is essential for the effective use of encryption. JCI will implement the following key management procedures to protect encryption keys from unauthorized access, loss, or compromise:

7.1 Key Generation

- Encryption keys will be generated using cryptographically secure methods and with sufficient randomness.
- Key generation processes will be performed in secure, controlled environments, such as using Hardware Security Modules (HSMs) or approved key generation software.
- The method of key generation must be documented.

7.2 Key Storage

- Encryption keys will be stored securely using strong access controls.
- Private keys for asymmetric encryption will be protected with the highest level of security.
- Hardware Security Modules (HSMs) or Key Management Systems (KMS) will be used where appropriate to enhance key security, especially for server-side keys.
- All keys, especially private keys, must be stored in an encrypted format.
- Keys stored in software must be protected with strong passwords or passphrases.

7.3 Key Distribution

- Encryption keys will be distributed securely using methods that prevent interception.
- Key exchange protocols will be employed to establish secure communication channels.
- Keys must only be distributed on a "need-to-know" basis.
- Electronic key distribution must be encrypted.

7.4 Key Rotation

- Encryption keys will be rotated periodically to reduce the impact of potential key compromise.
- Key rotation schedules will be defined based on the sensitivity of the data and the risk assessment. High-risk data should have more frequent key rotation.
- Key rotation procedures must be documented and automated where possible.

7.5 Key Backup and Recovery

- Secure backups of encryption keys will be maintained to ensure data recovery in case of system failures or disasters.
- Key recovery procedures will be documented and tested regularly.
- Backed up keys must be stored with the same level of security as the original keys.
- Access to backed up keys must be strictly controlled.

7.6 Key Destruction

- Encryption keys will be securely destroyed when they are no longer needed.
- Key destruction methods will ensure that the keys cannot be recovered or reconstructed. This may include using specialized software or physical destruction methods.
- Destruction of keys must be documented.

7.7 Key Access Control

- Access to encryption keys will be restricted to authorized personnel on a need-to-know basis.
- Access control lists will be implemented to manage key permissions.
- All access to encryption keys must be logged and monitored.
- Regular reviews of key access permissions will be conducted.

7.8 Responsibilities

- The IT Security team is responsible for the overall management of encryption keys, including establishing key management policies and procedures, and overseeing key lifecycle.
- Data owners are responsible for classifying their data and ensuring that encryption keys are used in accordance with this policy.
- System administrators are responsible for the secure storage and handling of encryption keys on their systems.

8 Data in Transit Protection

JCI will employ secure communication protocols and methods to protect data while it is being transmitted across networks and between systems.

8.1 Secure Protocols

- All data transmitted over public or untrusted networks must be encrypted using Transport Layer Security (TLS) protocol, version 1.2 or later. Secure Sockets Layer (SSL) is prohibited.
- All connections to JCI systems from untrusted networks must use a VPN.
- Secure protocols such as HTTPS, SFTP, and SSH will be used for secure data transmission.
- The specific version of TLS or other protocols must be the latest recommended version by NIST or other recognized standards bodies.

8.2 Email Encryption

- Sensitive information transmitted via email must be encrypted using S/MIME or other approved email encryption methods that provide end-to-end encryption.
- Employees are prohibited from sending unencrypted sensitive information via email over public networks.
- Email encryption should be enforced where technically feasible.

8.3 Secure File Transfer

- File transfer protocols such as SFTP (Secure FTP) or FTPS (FTP Secure) will be used for transferring sensitive files.
- Unsecured file transfer protocols such as FTP will not be used for transmitting sensitive data.
- File transfer systems must be configured to use strong authentication and encryption.

8.4 Virtual Private Networks (VPNs)

- Virtual Private Networks (VPNs) will be used to create secure, encrypted connections for remote access to JCI's network.
- All remote access to JCI's network must be conducted through an approved VPN.
- VPNs must be configured to use strong encryption and authentication.
- Split tunnelling should be avoided where possible or strictly controlled.

8.5 Wireless Network Security

- All wireless networks used to transmit sensitive data must be secured using strong encryption (e.g., WPA2/WPA3-Enterprise). WPA2/WPA3-Personal should be evaluated for risk.
- Weak or outdated wireless security protocols (e.g., WEP) are prohibited.
- Rogue wireless access points are prohibited.

8.6 Messaging Applications

- Business use of messaging applications for transmitting sensitive data must be approved by IT Security.
- Approved messaging applications must provide end-to-end encryption.
- Employees must be trained on the proper use of approved messaging applications.

9 Data at Rest Protection

JCI will implement encryption measures to protect sensitive data stored on various storage devices and systems.

9.1 Full Disk Encryption

- All laptops, desktops, and other portable devices used to store sensitive data must utilize full disk encryption (e.g., BitLocker, FileVault).
- Full disk encryption must be enabled and properly configured according to JCI's standards.
- The implementation of FDE must be verified.

9.2 File/Folder Encryption

- For specific files or folders containing sensitive information stored on shared drives or servers, encryption tools (e.g., EFS, VeraCrypt) will be used.
- Data owners are responsible for identifying and encrypting sensitive files and folders.

- File and folder encryption must be applied in a way that is transparent to authorized users.

9.3 Database Encryption

- Databases containing sensitive data will be encrypted at the database level or using Transparent Data Encryption (TDE) where supported by the database management system.
- Database administrators are responsible for implementing and maintaining database encryption.
- Database encryption keys must be managed according to the key management section of this policy.

9.4 Cloud Storage Encryption

- Data stored in cloud environments will be encrypted using encryption mechanisms provided by the cloud service provider, ensuring that JCI maintains control of the encryption keys whenever possible (e.g., Bring Your Own Key (BYOK)).
- JCI must approve the cloud provider's encryption methods and key management practices.
- Regular audits of cloud provider's security practices will be conducted.

9.5 Removable Media Encryption

- All removable media (e.g., USB drives, external hard drives) used to store sensitive data must be encrypted.
- Employees are prohibited from storing unencrypted sensitive data on removable media.
- JCI-approved encryption tools must be used for removable media.

9.6 Backup Encryption

- Backups of sensitive data must be encrypted to protect data in case of loss or theft of backup media.
- Backup encryption methods must be consistent with this policy and provide the same level of protection as the original data.
- Backup encryption keys must be managed according to the key management section of this policy.
- Regular testing of backup encryption and recovery procedures must be performed.

10 Policy Enforcement

Enforcement of this policy is critical to ensuring the protection of JCI's sensitive data.

10.1 Responsibilities

- The Office of Chief Information Security Officer (CISO) is responsible for developing, implementing, and maintaining this policy.
- Data owners are responsible for classifying their data and ensuring that their data is handled in accordance with this policy.
- All employees, contractors, and authorized users are responsible for complying with this policy.
- Managers and supervisors are responsible for ensuring that their staff are aware of and comply with this policy.
- Internal Audit is responsible for auditing compliance with this policy.

10.2 Non-Compliance

- Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract, and potential legal consequences.
- The severity of the disciplinary action will depend on the nature and severity of the violation.
- All instances of non-compliance must be documented.

10.3 Reporting Violations

- Any suspected violations of this policy must be reported to the Office of CISO immediately.
- Reports of violations will be investigated, and appropriate action will be taken.
- JCI will protect whistleblowers from retaliation.

11 Compliance

JCI is committed to complying with all applicable laws, regulations, and industry standards related to data protection and privacy. This policy is designed to support JCI's compliance efforts.

11.1 Relevant Regulations and Standards

- This policy is aligned with the requirements of regulations and standards such as:
    - Digital Personal Data Protection Act, 2023
- JCI will regularly review and update this policy to ensure ongoing compliance.
- JCI will conduct regular assessments to ensure compliance with relevant regulations and standards.

12 Regular Audits and Monitoring

JCI will conduct regular audits and monitoring to ensure the effectiveness of this encryption policy and to identify any potential vulnerabilities.

12.1 Audit Frequency

- Audits of encryption practices will be conducted at least annually.
- Additional audits may be conducted as needed, such as after a security incident or significant system change, or changes in regulations.
- Audits may be performed by internal or external auditors.

12.2 Audit Scope

- Audits will cover all aspects of this policy, including encryption methods, key management, and compliance.
- Audits may involve reviewing system configurations, logs, policies, procedures, and employee practices.
- Audits will assess the effectiveness of encryption controls.

12.3 Monitoring

- The IT Security team will monitor systems and networks to detect any unauthorized access or attempts to bypass encryption controls.
- Monitoring activities may include reviewing security logs, using intrusion detection systems, and security information and event management (SIEM) systems.
- Monitoring will be continuous where technically feasible.

12.4 Audit Reporting and Follow-Up

- Audit findings will be documented and reported to management.
- Corrective actions will be taken to address any identified deficiencies in a timely manner.
- Audit findings and corrective actions will be tracked and reviewed by management.

13 Incident Response

JCI has established an incident response plan to address security incidents, including those involving data breaches or key compromise.

13.1 Encryption in Incident Response

- Encryption plays a critical role in mitigating the impact of data breaches by rendering stolen data unreadable.
- In the event of a data breach, JCI will assess whether encryption was properly implemented and used.
- The incident response plan will include procedures for determining if encryption was defeated or bypassed.

13.2 Key Compromise

- If an encryption key is suspected of being compromised, immediate action will be taken to revoke the key and re-encrypt affected data.
- Procedures for key compromise will be documented in the incident response plan, including steps for identifying affected systems and data, and notifying affected parties.
- A post-incident review will be conducted to determine the cause of the key compromise and to prevent future occurrences.

14 Version Control

This policy will be reviewed and updated periodically, at least annually, to ensure its effectiveness and alignment with evolving security threats, technological advancements, and changes in applicable laws and regulations.

14.1 Version History

Version	Date	Author	Description of Changes	Approved By
1.0	30/05/2025	Prasenjit Saha, AM-IT	Initial version	Managing Director

14.2 Review and Approval

- This policy will be reviewed and approved by Head of the Department (IT), CISO, Director (Finance) and Managing Director.
- Changes to this policy will be communicated to all affected parties.

IT Asset Disposal Policy

Version 1.0

THE JUTE CORPORATION OF INDIA LIMITED (JCI)
PATSAN BHAWAN
ACTION AREA – 1, CF BLOCK
NEW TOWN
KOLKATA-700156

EFFECTIVE DATE: 01/06/2025
PLACE: KOLKATA

CONTENTS

1 PURPOSE

This policy establishes the procedures for the secure, compliant, and environmentally responsible disposal of obsolete, non-functional, or unneeded IT hardware and software assets owned or leased by The Jute Corporation of India Limited (JCI).

2 OBJECTIVES

The objectives of this policy are to:

- Ensure secure removal of data from all IT hardware prior to disposal, in accordance with ISO/IEC 27040 and IEEE 2883 standards for data sanitization.
- Comply with all applicable environmental and legal requirements for electronic waste disposal, including the E-Waste (Management) Rules, 2022 and any amendments.
- Prevent unauthorized use or distribution of software and licenses, ensuring compliance with licensing agreements.
- Maintain accurate asset records, including disposal details, for auditing and financial reporting compliance.

3 SCOPE AND APPLICABILITY

This policy applies to all JCI employees, including outsourced, contractual, and temporary employees, involved in the use, management, and disposal of IT assets owned or leased by JCI at all locations, including the Head Office, Regional Offices (ROs), Regional Office-cum-Lead DPCs (RLDs), and Departmental Purchase Centers (DPCs).

IT assets covered by this policy include, but are not limited to:

- Servers
- Personal Computers (PCs) and Dumb Terminals
- Printers, Scanners, Photocopier Machines, and Plotters
- Uninterruptible Power Supplies (UPS)
- Laptops, Notebooks, and Tablets
- Liquid Crystal Display (LCD) and Light Emitting Diode (LED) Displays
- Data Communication Equipment, including Local Area Network (LAN) switches, routers, and data cables
- Webcams and Speakerphones
- Biometric Devices
- Mobile devices
- Electronic devices
- Software (operating systems, applications, licenses)

Note: Consumable IT items, such as used printer cartridges, are excluded from this policy due to their nature as consumables. Petty-valued, non-capitalized IT items like pen drives and floppy disks are also excluded from the detailed scrapping procedure.

4 GROUNDS FOR DISPOSAL

IT assets may be disposed of under the following circumstances:

- **End of Useful Life:** The equipment has outlived its prescribed useful life, as certified by the IT Department, and is unfit for its intended purpose. The prescribed useful life for various IT equipment is as follows:
  - Servers/PCs/Dumb terminals/Monitors - 5 years.
  - Laptop/Notebook - 4 years or until the fitness of such device is certified by the IT team of the JCI, whichever is later.
  - UPS (excluding battery) - 5 years.
  - Battery of UPS - 1 year after the warranty period.
  - Printers/Scanners/Photocopier Machine/Plotter - 5 years.
  - Webcam, Speakerphone - till smooth working condition.
  - Data Communication Equipment/LAN switches/routers/data cables - 5 years.
  - Biometric Devices - 7 years.
  - Mobile device- 3 years.
  - Electronic device- 3 years.

Note: Equipment may continue to be used beyond the prescribed life if it meets user requirements and functions satisfactorily. The life of equipment not listed above shall be as per the report of the Original Equipment Manufacturer (OEM) or service engineer of the respective equipment.

- **Technological Obsolescence:** The equipment has become technologically obsolete, cannot be upgraded, vendor support is unavailable, and its use may result in security threats/unauthorized access to data.
- **Beyond Economical Repair:** When the repair cost exceeds 50% of the asset's residual value (calculated using a depreciation rate of 20% per year), making repair uneconomical. Such cases should be dealt with on a case-to-case basis and should have the concurrence of the Finance Department.
- **Damage:** The equipment has been damaged due to fire or any other unforeseen reason and has been certified as beyond repair by the authorized service agency and agreed upon by the IT team of JCI.

5 Disposal Procedures

5.1 Before Decommissioning

- All data should be backed up and securely stored within a secure location. JCI databases must be backed up.
- The device must be sanitized and verified for data wipeout to avoid any information leakage.
- All software must be uninstalled from the device in compliance with licensing agreements.

5.2 Disposal Methods

- **Donation:** The asset may be donated to verified charitable organizations with the appropriate approval from the designated authority. Due diligence must be performed to verify the legitimacy of the recipient organization, and proper documentation must be maintained.
- **E-waste Recycling:** The asset will be disposed of through certified e-waste recycling partners/vendors in compliance with the E-Waste (Management) Rules, 2022 and any amendments. Vendors must provide certification of their recycling processes.
- **Destruction:** Physical destruction (e.g., degaussing or shredding) will be used when data security is paramount, and data wiping is insufficient. The method of destruction will be appropriate to the type of media.

5.3 Software Disposal

- Software licenses must be uninstalled and deactivated upon decommissioning.
- Software license keys must be returned to the IT Department for potential reuse.
- Cloud or Software as a Service (SaaS) subscription must be terminated or transferred as applicable.

5.4 Approval and Documentation

- All disposals must be approved by the Head of the IT Department (or designated authority).
- A disposal form (Annexure I) must be completed for each asset, including asset ID, serial number, and reason for disposal.
- All disposals must be recorded in the IT Department's asset register.
- Certificates of destruction or recycling must be obtained from vendors and retained.

5.5 Procedure

- The user section will initiate the scrapping proposal, which the Material Section will compile for further processing.
- Each division will prepare an "IT equipment condemnation note" in the pro-forma attached as Annexure-I.
- JCI will constitute a Condemnation Committee to review the condemnation notes and

recommend the condemnation of equipment as per approved guidelines. The committee should have at least one member from the IT section and one from the finance section.

- The condemnation report so prepared shall be put up for approval. The condemnation will be done only after approval is obtained from the competent authority having such powers to approve condemnation. It is suggested that such Scrapping Committee will meet twice a year, during the months of May-June and Nov-Dec., to avoid piling up of unusable IT items.
- Once approved, the equipment will be removed from office use and stored in the area allocated for scrapped equipment.
- The department will ensure the removal of service and inventory labels from such equipment.
- Annual Maintenance Contracts (AMCs) for such scrapped equipment/instruments should be terminated with the effective date of scrapping.

6 Compliance and Security

- All disposals must comply with relevant data protection laws and regulations, including the E-waste (Management) Rules, 2016 and any amendments, and other applicable laws.
- Disposal partners/vendors must provide evidence of proper handling, data destruction, and recycling practices and certifications. JCI must vet and select disposal vendors based on their compliance and security practices.
- Non-compliance with this policy may result in disciplinary action and potential legal consequences.

7 Responsibilities

- **IT Department:**
  - Develop and maintain this policy.
  - Ensure secure data wiping and verification using approved methods.
  - Manage software licenses and ensure proper uninstallation.
  - Oversee the physical disposal of IT assets, including coordination with vendors.
  - Maintain accurate records of all disposals.
  - Provide guidance and training to other departments on this policy.
- **Finance Department:**
  - Ensure that disposals are accurately reflected in the fixed asset register.
  - Provide input on asset valuation and residual value calculations.
  - Maintain financial records related to asset disposal.
- **Employees:**
  - Adhere to the guidelines outlined in this policy.
  - Properly back up data before returning or disposing of IT assets.

- Return IT hardware and software promptly when no longer needed.
- Complete required disposal documentation accurately.

8 Version Control

This policy will be reviewed and updated periodically, at least annually, to ensure its effectiveness and alignment with evolving security threats, technological advancements, and changes in applicable laws and regulations.

8.1 Version History

Version	Date	Author	Description of Changes	Approved By
1.0	30/05/2025	Prasenjit Saha, AM-IT	Initial version	Managing Director

8.2 Review and Approval

- This policy will be reviewed and approved by Head of the Department (IT), Director (Finance) and Managing Director.
- Changes to this policy will be communicated to all affected parties.

This revised policy incorporates more detailed information, addresses a wider range of data protection scenarios, and emphasizes the importance of ongoing monitoring, auditing, and compliance.

ANNEXURE I:

IT EQUIPMENT CONDEMNATION NOTE

Part A: User Information

Name of User: _____

Designation: _____

Department: _____

Location: _____

Email ID: _____

Telephone No.: _____

Sr. No.	Item	Make & Model	Serial No. of Item	Reason for Scrapping
1				
2				
3				
4				
5				
6				

Signature of User: _____

Recommendation of HoD (IT): _____

Part B: Procurement Section Information

Sr. No.	Name of the Item with Serial No.	Date of Purchase	Purchase Cost as per Record	Asset/Stock Register Entry Page No.
1				
2				
3				
4				
5				
6				

Signature of Dealing Official: _____

Part C: Finance Division Information

Sr. No.	Name of the Item	Reason for Scrapping	Residual Value	Any Other Information/Remarks
1				
2				
3				
4				

Signature of Scrapping In-charge: _____