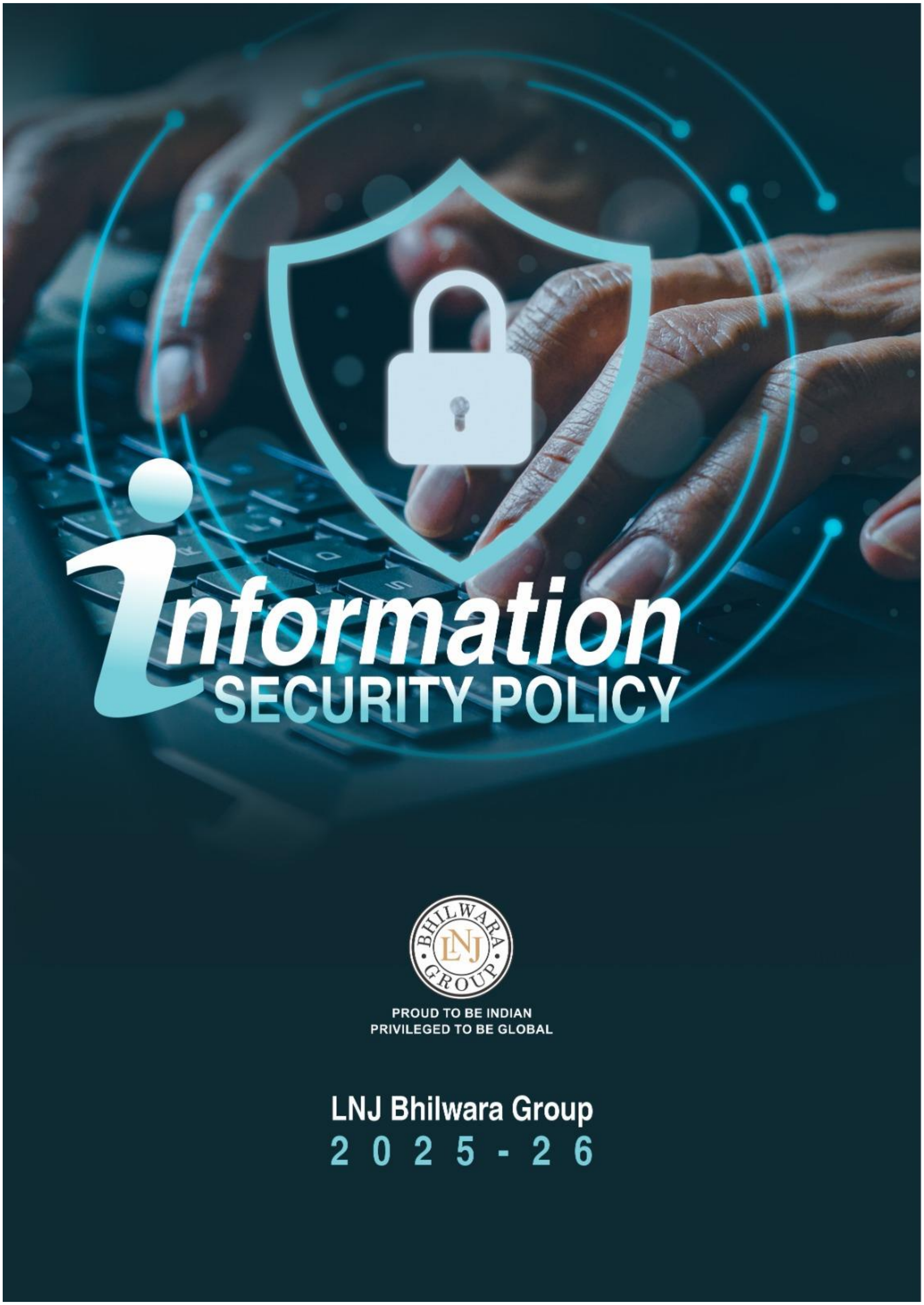

Information SECURITY POLICY

PROUD TO BE INDIAN
PRIVILEGED TO BE GLOBAL

LNJ Bhilwara Group
2025-26

Table of Content

1. Information Security Policy

Introduction

IT and the Internet are crucial for business success but also bring security risks. Protecting company data and systems is essential to safeguard intellectual property and ensure smooth operations.

Vision

Use IT to drive business growth while keeping information and systems secure.

Mission

Protect data, infrastructure, and applications by preventing, detecting, and responding to threats.

Objectives

This policy applies to all employees and aims to:

a) Secure business data (Confidentiality, Integrity, and Availability).

b) Meet legal and regulatory requirements.

c) Reduce risks from:

  I. Cyberattacks (hackers, malware).

  II. Accidents (system failures, disasters).

  III. Weaknesses (unpatched systems, poor security).

Key Focus Areas

- **Confidentiality:** Only authorized access to data.
- **Integrity:** Keep data accurate and systems reliable.
- **Availability:** Ensure systems and data are always accessible when needed.

2. E-mail Policy

2.1 Email ID Format

a. Unique email IDs in the format: <Firstname>.<Lastname>@<companydomain>.com. exception as per Group CIO approval.

b. No duplicates permitted (e.g., x.y1@lnjbhilwara.com if x.y@ exists).

c. Users must update **mobile numbers** and **personal email IDs** in their profiles for security alerts.

2.2 Email Client & Attachments

a. **HCL Notes** is the standard email client.

b. Users must **avoid** opening attachments/links from untrusted sources.

2.3 Email Usage

a. **Only company email** may be used for business communication.

b. Personal email accounts are prohibited for work-related correspondence.

2.4 Email Disclaimer, Signature & Security

a. **Disclaimer:** All outgoing emails must include:

"This email is confidential. If you're not the intended recipient, please delete it and inform the sender. LNJB does not guarantee the accuracy or safety of this message. Check for viruses before opening attachments."

b. Signatures must be **professional** (name, designation, contact details).

c. **Password resets** require identity verification via IT ticketing

2.5 Mailbox Size & Retention

a. **Lotus Notes users:**

- 45-day mail retention on servers.
- **25 MB limit** per sent/received email (including attachments).

b. Users must **archive older emails locally**.

c. IT performs **daily backups** (per **Section 15**).

2.6 Security & Data Protection

a. **Firewalls/email gateways** filter spam/malware.

b. **Antivirus/DLP tools** block infected attachments/leaks.

c. Report suspicious emails to cyber.alert@lnjbhilwara.com.

d. IT may **disable risky features** to protect the network.

2.7 Prohibited Actions

No **abusive, discriminatory, or non-business emails**.

b. **No unauthorized access**, spam, or auto-forwarding (exceptions require **BH/COO/Group CIO approval**).

c. **"Reply All"** must be used cautiously.

d. Auto forwarding to personal id is strictly prohibited

e. **Passwords must not be shared**.

2.8 Compliance & Logs

a. Email logs may be disclosed to **law enforcement** per government regulations.

3. Access Control Policy

3.1 User Access Review for Applications and Systems

a. Quarterly review:

- IT generates **Active Directory user reports**,
- Shares with location IT Heads for review.

b. **Functional managers/HODs must:**

- Validate appropriateness of access,
- Confirm via email within **3 weeks**.

c. For changes/deletions, functional managers coordinate with IT.

d. Disabled/locked IDs require **functional manager approval** for reactivation.

e. Inactive accounts (>90 days) shall be **disabled** (approved by HOD/Group CIO).

3.2 User ID Security Controls

a. Disable **default vendor IDs** in hardware/software.

b. Account lockout:

- After **5 failed password attempts**,
- Auto-unlock in **30 minutes**.

c. Non-domain apps: Users contact IT for unlocks/password resets.

d. Device auto-lock: 10 minutes of inactivity.

e. IT ensures **accurate clock settings** on all devices:

- Users cannot modify,
- Critical for audit logs/legal compliance.

f. Critical business data must be stored on **dedicated shared drives** by user

4. Anti-Virus Policy

4.1 Management of Anti-Virus Software

a. Users are restricted from disabling antivirus software.
b. On access scan should be enabled

c. Anti-spam/antivirus filters must block malicious emails before delivery.
d. Infected systems must be isolated until verified as virus-free.

4.2 Best Practices for Virus Prevention

a. Do not forward spam/chain/junk emails (potential virus carriers).
b. Avoid opening files, links, or macros from unknown/untrusted sources.
c. Location IT Heads must monitor and resolve antivirus compliance issues via the console.
d. IT shall train users on virus threats and safe practices (e.g., avoiding suspicious links/attachments).
e. Antivirus logs must retain 90 days of data for tracking unauthorized access or virus incidents.

5. Password Management Policy

5.1 User Password Management (Active Directory Domain Services)

a) **Password Complexity:** Must include alphanumeric + special characters, with at least one uppercase and one lowercase letter.
b) **Minimum Length:** 9 characters.
c) **Password Expiry:** Mandatory change every **90 days**.
d) **Password History:** Last **3 passwords** cannot be reused.

e) **Account Lockout:** After **5 failed attempts**, display "Account locked."

f) **First Login:** Users must change default passwords immediately.

g) **Expiry Notification:** Alert users **10 days** before password expiry.

h) **Account Unlock/Password Reset:** Contact IT for assistance.

i) **Secure Storage:** Passwords must **not** be stored in plaintext (scripts, browsers, etc.).

j) **Temporary Sharing:** If shared for external support, change immediately after use.

k) **Password Change:** Requires both old and new password.

5.2 Privileged/Super User Password Management

a) **Usage:** Only for system/configuration changes (approved via change management).

b) **Restriction:** No administrator access for daily operations.

c) **Secure Storage:** All privileged passwords must be **vaulted**.

d) **Regular Updates:** IT must ensure periodic password changes to maintain accessibility.

6. Incident management policy

6.1 Incident Management Practice Standard

a. The IT Department is responsible for handling all IT and security-related incidents within LNJB Group.

b. For any suspected or confirmed security incident (e.g., malware, phishing, unauthorized data access, hacking tools, etc.), the following procedure must be followed:

i. **Reporting**: Notify the IT Department immediately via email, phone, or IT Service Management tool by logging an incident.

ii. **Response**: The designated IT team/personnel will analyze and initiate corrective actions, including restoration, per established guidelines.

iii. **Resolution Time**: Incident response and resolution timelines will align with the severity,

iv. **Mitigation**: IT shall repair damages, mitigate risks, and eliminate/minimize vulnerabilities.

v. **Escalation**: The **Head of Department/Group CIO** will report the incident to management and communicate updates to affected users.

vi. **Post-Incident Review**: A root cause analysis (RCA) and corrective actions must be documented and shared with the **Group CIO** and relevant teams to prevent recurrence.

7. Cyber Risk Policy

At LNJ Bhilwara Group, we prioritize the protection of our digital assets and the confidentiality, integrity, and availability of sensitive information. This Cyber Risk Policy establishes key principles that all employees must adhere to in order to mitigate cybersecurity risks.

Key Policy Principles

7.1 Responsibility and Awareness

- All employees are responsible for understanding and complying with the Cyber Risk and IT Security Policy.
- Regular cybersecurity training will be conducted to enhance employee awareness and preparedness.

7.2 Password Security

- Strong, unique passwords are mandatory to prevent unauthorized access.
- Passwords must not be shared and should be updated periodically.

7.3 Phishing and Social Engineering

- Employees must exercise caution with unsolicited emails, links, or requests for sensitive information.
- Always verify sender authenticity before responding to or acting on such communications.

7.4 Device Security

- All company-issued devices (computers, smartphones, tablets) must be kept updated with the latest security patches.
- Only company-approved security software may be installed.

7.5 Remote Work Security

- The IT department will ensure secure VPN connectivity for remote access.
- Public Wi-Fi networks must be avoided for business-related tasks.

7.6 Third-Party Risk Management

- Sensitive information may only be shared with external vendors/partners after signing a Non-Disclosure Agreement (NDA).

7.7 Social Media and Online Conduct

- Employees must refrain from disclosing work-related or sensitive company information on social media.

7.8 Compliance

- Adherence to industry regulations and internal cybersecurity policies is mandatory.
- Non-compliance may result in disciplinary action.

8. Data Classification policy

Information shall be disclosed only to authorized personnel with a legitimate business need, following a **"need-to-know"** principle to prevent unauthorized access, modification, or deletion.

8.1 Data Handling:

- Share information only with authorized personnel who need it. Follow the **"need-to-know"** rule.

8.2 Information Assets:

- Identify and track important assets like:
    - **Data** (contracts, databases, backups)
    - **Software** (OS, tools)
    - **Hardware** (laptops, servers)

  - **People & Services** (employees, vendors)

8.3 Data Classification Levels:

Level	Definition	Examples
Restricted	Very sensitive; high risk if leaked	Trade secrets, customer data
Confidential	Sensitive; could harm the company	Audit reports, marketing plans
Internal	For employees only; low risk if leaked	Training docs, company directory
Public	Safe to share publicly	Ads, press releases

8.4 Key Rules:

- Classify data based on **importance (CIA: Confidentiality, Integrity, Availability)**.
- Employees must follow classification guidelines.

8.5 Changing Classification:

- Only **Information Owners** can lower a classification (e.g., from Confidential to Internal).

8.6 Keeping Data Safe:

- **Do NOT:** Share confidential data, copy without permission, or misuse systems.
- **Confidential Data Includes:** Contracts, financial reports, employee details, strategies.
- **Violations = Disciplinary action.**

9. Data Centre and Network Security Policy

9.1 Remote Access Connectivity

a. **Approved Tools Only**: Remote access requires IT-authorized software.
b. **HoD Approval**: Functional heads must authorize access requests.
c. **Credential Management**: As per AD approved list by CIO/HOD/Plant Head.
d. **Incident Reporting**: Users must report breaches immediately to IT and managers.
e. **Daily report:** Remote access lists should be shared with Group CIO on daily basis.