CYBER SECURITY POLICY

OF

APOLLO PIPES LIMITED

Version	Revision Date	Approved by	Date of Approval
1st Version		Board of Directors	25.07.2023
2nd Version	26.10.2023	Board of Directors	26.10.2023
3rd Version	05.11.2026	Board of Directors	05.11.2026

I. Objectives

Apollo Pipes Limited ("the Company") is committed to safeguarding the confidentiality, integrity, and availability of its information assets. This Information Security Policy ("Policy") establishes the principles and governance framework for protecting information and information systems against cyber threats, data breaches, misuse, and unauthorized access.

- Protect business-critical, personal, and confidential information.
- Ensure resilience of IT and operational technology (OT) systems.
- Comply with applicable legal, regulatory, and contractual requirements.
- Support enterprise risk management and ESG governance expectations.

II. Applicability and Scope:

This policy applies to:

- All employees, contractors, consultants, and third parties involved in data generation, processing, validation, or reporting.
- All information assets, including data, applications, infrastructure, and networks.
- Operational Technology (OT) systems at manufacturing plants.
- All systems, digital platforms, documents, and data repositories that are used for Sustainability & Governance Reporting.
- Third-party service providers handling Company information.

III. Governance And Oversight

- Information security is treated as an enterprise-wide risk and forms part of the Company's overall risk management framework.
- The Board of Directors / Risk management Committee / Audit Committee provides oversight on cyber and information security risks.
- The CIO is responsible for implementation and maintenance of information security controls.
- Senior Management periodically reviews cyber risk posture, incidents, and mitigation plans.

IV. Policy Principles

A. Creating a Secure Cyber Ecosystem

1. Designate a Cyber Security Organization Structure under IT Chief to coordinate all matters related to cyber security in Company, with clearly defined roles and responsibilities for all stakeholders in Offices/ Divisions.

2. Develop relevant information security policies duly integrated with their business plans and implement such policies aligning with the best practices. These policies may include advisories received from various agencies like CERT-In, Cyber Security Group (MoD), Cyber Information Research Agency towards compliance requirements.

3. Allocate specific Capital and Revenue Budgets towards implementing cyber security initiatives and meeting emergency response arising out of cyber incidents.

4. Encourage stakeholders to install, upgrade and strengthen information infrastructure towards better prepared cyber security posture.

5. Ensure data privacy by strictly limiting data access on need-to-know basis. Keep the personally identifiable information (PII) e.g., Aadhaar Number, PAN Number, Bank Account Number, Passport Number etc. is stored with adequate security measures and access restrictions.

7. Third-Party And Vendor Security

- Third parties handling Company data must comply with defined information security requirements.
- Cyber security clauses shall be included in relevant contracts.
- The Company reserves the right to review and audit third-party security practices.
- Vendor access shall be revoked upon termination of engagement.

8. Role Specific Responsibilities

- All employees, contractors, and relevant third parties shall be responsible for complying with the Company's information security requirements and for safeguarding information assets in accordance with their assigned roles and responsibilities.

Role	Responsibilities
All employees	Understand and follow this policy; complete cyber security awareness training at joining and annually; report incidents promptly.
Managers and Department Heads	Ensure team members follow this policy; approve access only on a need-to-know basis; request removal of access when people move roles or leave; ensure training is completed.
Business Heads	Are accountable for compliance within their business areas; ensure security requirements are built into business processes and projects.
IT Security team	Maintain security controls and monitoring; manage incident response; run awareness programmes; review access and compliance periodically.
IT and OT system administrators	Use privileged accounts only for administrative tasks; apply patches and secure configurations; maintain backups; keep logs of changes.
HR	Include policy acceptance in onboarding; inform IT promptly of joiners, movers and leavers; support disciplinary action for violations.
Vendors, contractors and	Sign confidentiality and security undertakings; follow this policy while

third parties	using Apollo Pipes Ltd systems or data; report incidents immediately; return or destroy data at contract end.

B. Creating an Assured Framework

1. Adopt global best practices to the maximum extent feasible in information security and compliance and thereby enhancing cyber security posture.

2. Create infrastructure complying with conformity assessment and requirements as mandated by various adopted International Standards, Internal System Audits, Vulnerability Assessment and Penetration Testing (VAPT) by CERT-In Empanelled Auditors etc.

3. Enable implementation of global security best practices in the formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all concerned.

4. Identify and classify information infrastructure facilities and assets at entity level considering risk perception for undertaking commensurate security protection measures, such as separation of private and public networks etc.

5. Encourage secure application/ software development processes complying with the known best practices.

6. Create conformity assessment framework for periodic verification of compliance to standard, guidelines, audit observations and other adopted benchmarks on cyber security.

7. Encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and accordingly take steps for periodic patching/ upgrade.

C. Strengthening the Compliance Framework

1. Mandate periodic audit and evaluation of adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to CSG (DDP/MoD) Guidelines.

2. Enable, educate and facilitate awareness of the Cyber Security Guidelines.

3. Ensuring appropriate physical, logical, and procedural controls are in place to preserve confidentiality, integrity, availability and privacy of information.

D. Data Management Controls

a) <u>Data Collection</u>

- All data must originate only from authorized, approved data sources.
- IoT/automated data systems must have calibration and audit trails.

b) <u>Data Storage</u>

- All information shall be stored only in designated secure systems approved by IT.
- Data must be backed up as per the enterprise backup policy.

c) <u>Data Access</u>

- Role-based access control (RBAC) must be enforced.
- Access is granted only on recommendation of the data owner and IT approval.
- All access privileges shall be reviewed quarterly.

d) <u>Data Transmission</u>

- Data shared externally must be approved by the Steering Committee.
- All transfers must use secure channels (VPN, HTTPS, SFTP, or encrypted email).

e) Data Retention

- Archival must follow Information Lifecycle Management (ILM) standards.
- All records shall be retained for minimum 8 years or as required by statutory/regulatory requirements.

The Company is committed to protecting personal and sensitive data in line with applicable laws and regulations.

E. Creating mechanisms for security threat early warning, vulnerability management and response to security threats

1. Create systems, processes, structures and mechanisms to generate necessary situational scenarios of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions.

2. Cooperate and coordinate with National Level Computer Emergency Response Team (CERT-In) in dealing with National Cyber Crisis Situations.

3. Implement Cyber Crisis Management Plan towards dealing with cyber incidents adversely impacting critical processes or endangering safety and security.

4. Conduct and facilitate regular cyber security drills/ audits/ exercises to enable assessment of the security posture and level of preparedness in resisting and dealing with cyber security incidents.

5. Adopt advanced techniques and solutions towards enhancement in degree of data protection.

F. Incident Response Plan

Phase 1: Detection & Analysis, it's crucial to establish a Security Incident Response Team with diverse expertise, including representatives from management, technical, legal, and communications disciplines. External experts should be brought in if necessary. This team will create a plan, acquire necessary tools, and, when an incident occurs, act swiftly to address it.

Phase 2: Detection & Analysis, involves recognizing event signs, analyzing detected signs, documenting the incident, prioritizing it based on its potential impact and notifying relevant departments. A well-prepared incident response plan should outline reporting procedures.

Phase 3: Containment aims to limit the incident's impact and includes assessing severity, root cause analysis, identifying affected systems and data, ensuring legal compliance, maintaining business continuity, developing a communication strategy, classifying the incident, allocating resources, and defining timelines. Documentation is vital for learning from the incident and potential litigation preparation.

Phase 4: Eradication & Recovery, the response may include isolating and quarantining compromised systems, investigating the root cause, applying patches, removing malware, changing credentials, enhancing security measures, reviewing and updating policies, restoring data, validating systems, communicating with users, and implementing monitoring and surveillance. Detailed records of actions taken are essential for future analysis and reporting.

In Phase 5: Lessons Learned, a comprehensive post-incident review should be conducted to identify areas for improvement. This includes communication and reporting, ongoing security enhancements, and sharing final findings with relevant authorities such as CERT-In and SEBI.

G. Sensitization of Human Resource on Cyber Security

1. Mandate cyber security training infrastructure through Computer Based Training

2. Facilitate cyber security training for Cyber Security Professionals.

3. Maintain records of general awareness assessment, professional training on cyber security and knowledge base adequacy assessment on Cyber Security

H. Creating Cyber Security Awareness

1. Promote a comprehensive companywide awareness program on security of cyberspace through continual and effective communication (e.g. Newsletters).

2. Sustain security awareness and publicity campaign through electronic media such as companywide screensavers.

3. Conduct, support and enable cyber security workshops / seminars and certification.

Reporting

Company shall ensure transparent reporting of all cybersecurity incidents by aligning their reporting procedures with internationally recognized frameworks.

Review and Amendment

This Policy shall be periodically reviewed by the Board of Directors and timely updated as per the necessity.