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

CYBER SECURITY POLICY

I. Objectives

1. To create a secure cyber ecosystem, generate adequate trust and confidence in the IT systems and transactions carried out in the cyberspace, and thereby achieving adoption of IT in all business process.

2. To create an assured framework for design of security policies, enabling compliance to global security standards, and deploying best practices identified through conformity assessment (product, process, technology and people).

3. To develop/ deploy suitable security technologies towards achieving Secured ICT Assets meeting Company's overall security requirements.

4. To enable protection of information while in process, handling, storage and transit so as to safeguard privacy of personal and sensitive data and avoiding economic losses primarily due to cyber-crime or data theft.

5. To encourage the culture of alert and responsible behavior towards cyber security from all users through continual and effective communication.

II. Applicability and Scope:

On Apollo Pipes Limited and its subsidiaries (if any).

III. Need:

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, man-made or natural, and the data exchanged in the cyberspace can be exploited. The growth and penetration of IT systems has exposed them to varied threats emanating from internal and external sources. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting the functioning of critical information systems. Protection of information infrastructure and preservation of confidentiality, integrity and availability of information in cyberspace is the essence of a secured cyber space. Apollo Pipes Limited (the "Company") has adopted Cyber Security Policy as detailed below as an umbrella framework for defining and guiding the initiatives and reactive measures towards secured cyberspace.

IV. Strategies & Steps

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.

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. 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.

E. Incident Response Plan

In the first phase, 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.

F. 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

G. 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.

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

Company will 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.