POCL®

PONDY OXIDES AND CHEMICALS LIMITED

CYBERSECURITY POLICY

CYBERSECURITY POLICY

1. PURPOSE

The purpose of this Cybersecurity Policy is to establish a comprehensive framework for protecting the digital assets, information systems, manufacturing infrastructure, and sensitive business data of Pondy Oxides and Chemicals Limited (POCL) against cyber threats, unauthorized access, data breaches, and operational disruptions.

This policy aims to ensure business continuity, safeguard intellectual property, maintain stakeholder trust, and support secure and resilient operations across all business functions.

2. SCOPE

This policy applies to:

- All employees, directors, consultants, contractors, temporary staff, and third-party vendors associated with POCL.
- All company-owned, leased, or managed devices, systems, applications, networks, and cloud services.
- All manufacturing and operational technology (OT) environments, including but not limited to SCADA systems, PLCs, DCS, IoT devices, and industrial control systems.
- All data created, stored, transmitted, or processed by POCL, irrespective of format or location.

3. OBJECTIVES

The objectives of this policy are to:

- Protect manufacturing and business operations from cyberattacks, malware, ransomware, and unauthorized disruptions.
- Ensure confidentiality, integrity, and availability of organizational data and systems.
- Minimize cybersecurity risks through preventive and detective controls.
- Comply with applicable legal, regulatory, and contractual obligations.
- Promote cybersecurity awareness and accountability among employees and stakeholders.
- Establish effective incident detection, response, and recovery mechanisms.

4. ROLES AND RESPONSIBILITIES

4.1 Board / Senior Management

- Approve cybersecurity strategy, policies, and governance structure.
- Ensure adequate funding and resources for cybersecurity initiatives.
- Periodically review cyber risk posture and mitigation measures.

4.2 IT & Information Security Team

- Implement, monitor, and maintain cybersecurity controls.
- Conduct vulnerability assessments, risk reviews, and incident investigations.
- Manage backups, patching, endpoint security, and access controls.
- Respond to and remediate cybersecurity incidents.

4.3 Department Heads

- Ensure policy compliance within their departments.
- Identify critical systems and operational risks.
- Support cybersecurity awareness and training.

4.4 Employees

- Follow all cybersecurity procedures and safe computing practices.
- Protect credentials and company data.
- Report suspicious emails, devices, or activities immediately.

4.5 Vendors / Third Parties

- Comply with contractual cybersecurity requirements.
- Protect POCL data and systems from unauthorized access.
- Promptly notify POCL of security incidents affecting shared environments.

5. POLICY REQUIREMENTS

5.1 Access Control

- Access to systems and data shall be granted strictly based on business need and job role (Principle of Least Privilege).
- Strong passwords must be used and changed periodically.
- Multi-Factor Authentication (MFA) shall be enabled for critical systems and remote access.
- User accounts must be reviewed periodically.
- Access for terminated employees or expired contractors must be revoked immediately.

5.2 Device and Network Security

- All endpoints must have approved antivirus, anti-malware, and firewall protection.
- Operating systems and applications must be patched regularly.
- Network segmentation must be implemented between corporate IT and OT/manufacturing networks.
- Unauthorized devices shall not connect to POCL networks.
- Secure remote access methods (VPN/Zero Trust controls) shall be enforced.

5.3 Data Protection

- Sensitive data must be classified and handled according to business criticality.
- Confidential data must be encrypted both at rest and during transmission.
- Critical business and production data must be backed up daily.

- Backup restoration testing must be performed periodically.
- Use of removable storage devices (USB, external drives) shall be restricted and monitored.

5.4 Manufacturing Systems Security

- Industrial control systems including PLCs, SCADA, and IoT devices must be protected from unauthorized access.
- Default passwords must be changed before deployment.
- Unused services, ports, and protocols must be disabled.
- Production systems shall be monitored for anomalies or unusual behavior.
- Maintenance access to OT systems shall be controlled and logged.

5.5 Email and Communication Security

- Company email shall be used for official business communication.
- Confidential information shall not be shared through personal email or unauthorized messaging platforms.
- Employees must remain vigilant against phishing, spoofing, and social engineering attacks.
- Email filtering and threat detection controls shall be maintained.

5.6 Incident Response

- All suspected cybersecurity incidents must be reported immediately to the IT Security Team.
- POCL shall maintain an Incident Response Plan (IRP) with defined roles and escalation procedures.
- Incidents must be documented, investigated, and resolved promptly.
- Root cause analysis shall be performed to prevent recurrence.

5.7 Training and Awareness

- All employees shall undergo mandatory cybersecurity awareness training annually.
- Specialized training shall be provided for personnel managing critical manufacturing systems.
- Periodic phishing simulations and awareness campaigns may be conducted.
- Emerging cyber threats and advisories shall be communicated regularly.

5.8 Business Continuity and Recovery

- Critical systems must have disaster recovery and business continuity plans.
- Recovery objectives for essential operations must be defined.
- Recovery procedures shall be tested periodically.

5.9 Compliance and Audit

POCL shall align cybersecurity practices with recognized standards and applicable regulations, including:

- NIST Cybersecurity Framework
- Applicable Indian IT and data protection regulations

Regular audits, vulnerability assessments, and penetration testing shall be conducted to verify compliance and control effectiveness.

6. ENFORCEMENT

Violation of this policy may result in disciplinary action, including suspension of access privileges, termination of employment or contracts, and legal action where applicable.

Any intentional compromise of company systems, data, or security controls shall be treated as a serious offense.

7. POLICY REVIEW

This policy shall be reviewed at least annually or whenever significant changes occur in technology, business operations, threat landscape, or regulatory requirements.

All revisions must be approved by Board of Directors.