Paradeep Phosphates Limited (PPL)

Information Security Policy

Disclaimer:

This document is part of the information security policy of Paradeep Phosphates Limited (PPL), and shall not be used, circulated, quoted or otherwise referred to for any other purpose without prior written consent from PPL's information security committee.

Purpose:

Paradeep Phosphates Ltd. (PPL) recognizes that information is a critical business asset, and it should be protected from loss, theft, misuse, destruction, unauthorized access and modification. PPL is hence committed to safeguarding its information systems and assets, digital infrastructure, and data systems from intentional and unintentional unauthorized access and modification, misuse, loss, theft, or destruction internal or external to the organization.

This policy outlines the principles and responsibilities for ensuring confidentiality, integrity, and availability of information across all levels of the organization. It promotes secure, ethical, and lawful use of its information systems by employees, contractors, supply chain partners, and third parties.

Scope:

PPL has established a robust information security policy and governance mechanism to address availability, concerns, incidents related to information assets. This policy applies to:

- All employees, contractors, consultants, supply chain partners, and third-party service providers (collectively referred as stakeholders).
- All information systems, applications, networks, and data owned or managed by PPL.
- All physical and digital assets that are used to store, process, or transmit information.

Key Principles/ Measures:

PPL is committed to maintaining robust information security practices across its business operations and stakeholders by enforcing appropriate principles/ measures given as follows:

Acceptable Use of Assets

PPL's information systems and assets shall be used solely for collection through legal means, evaluation, reporting of data and information relating to PPL's business operations. Any use of information, information systems and assets owned or controlled by PPL for any direct or indirect personal use is strictly prohibited.

Data Classification and Handling

Information shall be classified as Public, Internal, Confidential, or Restricted. Confidential and restricted information shall be encrypted and shared only with authorized personnel. Any attempt to access the information outside the information security classification/ authorization levels is strictly prohibited unless such an attempt or use is explicitly approved by the owner of the information.

Access Control

Access to information systems and data shall be based on the principle of least privilege. Multi-factor authentication shall be enforced for all digital information systems and assets. Access rights shall be reviewed periodically and updated upon role changes or exit.

Asset Protection

All assets, servers, and mobile devices shall be protected with updated antivirus and firewall systems. Unauthorized software and hardware shall be restricted for download and usage on PPL's information systems and assets. PPL's information shall not be uploaded on any free online software or platform or file sharing websites unless approved by the information security committee.

Network Security and Internet Usage

Network traffic shall be monitored for anomalies and threats. Applications shall be tested for vulnerabilities before deployment. Emails shall be scanned for malware and phishing attempts. Internet usage shall be governed by acceptable use guidelines. Regular backups shall be performed for critical systems and information only on assets owned or controlled by PPL. Backup data shall be stored securely and tested periodically for recovery.

Incident Management

All security incidents shall be reported immediately to the IT Security Team. A formal incident response plan shall be activated for containment, investigation, and recovery. To raise any concern regarding information technology, cybersecurity, data privacy, individuals can send an email to dpmohanty@adventz.com and sanjitmohapatra@adventz.com.

Implementation and Governance:

PPL has established a working-level team or Risk Management Committee under the leadership of Mr. Dipankar Chatterji, which is responsible for implementation and monitoring of the policy. The team's key roles and responsibilities include:

- identification, evaluation, predication, and mitigation of risks and incidents
- review compliance status periodically (monthly basis)
- oversee the use and maintenance of information assets (digital as well as physical)
- enhance security measures and ensure continuous improvement to match requirements, technology, regulations.

Process and Infrastructure:

- Connectivity between Data Center (DC) and Disaster Recovery (DR) sites is secured through an MPLS VPN, reinforced by a firewall. External Internet Leased Lines (ILL) are also terminated at this firewall for added security.
- Utilization of Office 365 with point-to-point encryption, hosted on the Microsoft India cloud.
- Robust antivirus protection is installed on all endpoint devices to safeguard our network.
- SAP ERP system is integrated across all departments, enhancing efficiency in functions across departments sales, distribution, material management, finance, and HR.
- Regular monthly assessments of information assets (digital and physical) are conducted. These include credential management, data backup, and mock drills. To ensure external validation of

its systems, PPL undergoes an annual ITGC audit by external auditors, reviewing its information technology infrastructure and information security management systems. Additionally, PPL conducts yearly third-party Vulnerability Assessment and Penetration Testing, including simulated hacker attacks, to proactively identify and address vulnerabilities.

- Incident response procedures are shared with everyone to quickly restore operations in case of disruptions.

Training and Awareness:

Training programs related to information security shall be scheduled as a part of new recruitment orientation and ongoing training programs for existing employees. Participation in these training programs shall be tracked to ensure comprehensive engagement across the organization.

Any instance where an employee violates information security protocols shall be taken into account during the annual performance review process. Adherence to the principles is crucial and employee involvement in any violations could lead to disciplinary actions.

Compliance, Review, and Amendment:

This policy aligns with ISO 27001 international standard on information security management and other applicable Indian laws and regulations, and industry practices. The policy shall be reviewed annually or upon significant changes in technology, business operations, government regulations, or information security related incidents observed.

Internal Policy References:

- PPL's Privacy Policy
- Adventz Agri-business' Information Security Management System Policy

This policy version has been formally adopted by the organization following ratification by the ESG Steering Committee, led by the MD and all functional heads, and is currently in the process of getting endorsed by the Committee/ Board