PUNJAB CHEMICALS
AND CROP PROTECTION LTD.

CYBER SECURITY POLICY

CIN NO.: L24231PB1975PLC047063
Regd. Office: Milestone 18, Ambala Kalka Road, Village & P.O.: Bhankharpur,
Derabassi, Distt. S.A.S. Nagar (Mohali), Punjab-140201
Tel.: 01762-280086/ 280094 Fax: 01762-280070
Email :info@punjabchemicals.com Website: www.punjabchemicals.com

Objective:

Information is one of the most important asset for the strong foundation of the Company and is most essential for its business operations and effective customer services. Business units and functions shall implement adequate security policies, processes, and controls to protect confidentiality, maintain integrity, and ensure availability of all information assets.

Punjab Chemicals and Crop Protection Limited (PCCPL) is committed to establish and improve cyber security framework to minimize its exposure to various risks and safeguard PCCPL assets to achieve following goals:

- Consistently meet and exceed expectations of stakeholders and customers.
- Empower employees through training and awareness.
- Comply with the applicable international and national cybersecurity standards and regulatory requirements.
- Apply effective risk management to identify and treat current and emerging risks attached to PCCPL's business operations.
- Protect stakeholders, information and assets from threats that could disrupt business operations or damage the brand and reputation of Company.
- Implement efficient business continuity and disaster recovery management controls.
- Ensure compliance with all applicable legal, regulatory and contractual requirements to protect the Company's financial health and preserve its brand image and reputation.

Scope:

This policy applies to all stakeholders, who access PCCPL Information or networks including:

1. Full time employees and off-roll employees, - subsidiary staff, contractors, consultants, interns, temporary staff affiliated with third parties, including system vendors and staff from outsourcing companies.
2. This policy also applies to all - computer and data communication systems, information and infrastructure owned, licensed, or administered by PCCPL or its service providers and covers all other information of PCCPL.

Policy Commitments:

a) Risks to information and cyber systems shall be identified and mitigated to an acceptable level through a formal, documented procedure.
b) Critical information shall be protected from unauthorized access, use, disclosure, modification, or disposal- whether intentional or unintentional.
c) The confidentiality, integrity and availability of - information acquired permanently or in transit, provided or created shall always be ensured.
d) All Business and Department Heads are directly responsible for ensuring compliance with this information security policy in their respective business domains.
e) All actual or suspected breaches of information security including those involving employee related information shall be reported and investigated by the designated personnel and appropriate corrective and preventive actions shall be

Initiated.

f) Awareness programs on Information Security shall be provided to employees and wherever applicable to third parties. Annual training shall be conducted to all stakeholders.
g) The Business Continuity Plan shall be maintained and periodically tested for business critical information assets.
h) PCCPL shall collaborate with cyber security and data privacy experts to continually enhance its information management infrastructure.
i) All audit, legal, statutory, regulatory, and contractual requirements related to Information security shall be met wherever applicable.
j) The policy shall be reviewed periodically to ensure its effectiveness and relevance in light of technological changes evolving Risk Levels that may have impact on Confidentiality, Integrity and Availability, legal and contractual requirements, and business efficiency.
k) Vulnerability assessment and penetration testing (VAPT) shall be conducted periodicity either internally or through external party.

Compliance:

It is the responsibility of all employees to understand and adhere to the Information Security Policy.

Non-compliance or violation of this policy shall result in the invocation of PCCPL consequence management policy. Policy non-compliances by off-roll employees will be referred to the relevant functional/ Dept. head for appropriate actions as per procurement/ legal norms and rules to be taken up with the concerned Vendor/partner. PCCPL Management reserves all rights to take disciplinary action in case of its violation.

Review:

This policy shall be reviewed annually to access its effectiveness and relevance in light of technological changes evolving risk levels that may impact privacy, legal & contractual requirements, and business efficiency.

Any changes/modifications in this policy can be made by the IT team and they are responsible for the implementation of the policy.