PRIVI SPECIALITY CHEMICALS LIMITED

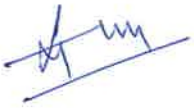
CYBER SECURITY POLICY

INFORMATION TECHNOLOGY

DOCUMENT CODE. POL-IT-003 Version:0.1 Date: 29/01/2025

Document Version Control				
Issue Date	**Version**	**Prepared By**	**Reviewed By**	**Approved By**
20-02-2024	V0.0	Mr. Kailash Nitore	Mr. Sachin Jadhav	Mr. Krishna Parab
29- 01-2025	V0.1	Mr. Kailash Nitore	Mr. Sachin Jadhav	Mr. Sachin Rajurkar

SIGNATURE PANEL OF APPROVAL

Name	Function	Date of Signature	Signature
Preparation			
Mr. Kailash Nitore	Manager-Infrastructure and Security	27-01-2025	
Review			
Mr. Sachin Jadhav	Asst. General Manager Infrastructure and Security	28-01-2025	
Approver			
Mr. Sachin Rajurkar	IT Head of the Department	29-01-2025	
Supersedes			
There are no changes.			

SUMMARY OF CHANGES

CHANGE HISTORY				
Rev.	**Doc Ref/Type.**	**Details of Changes**	**Effective**	**Originator**
0.1	**Document**	**No change**	**29- 01-2025**	**Sachin Jadhav**

INDEX

Contents

1. **PURPOSE** 5
2. **OBJECTIVES** 5
3. **SCOPE** 6
4. **ROLES AND RESPONSIBILITIES** 6
5. **POLICY STATEMENT** 6
6. **ACTIVITIES/RECORDS TO BE MAINTAINED** 11
7. **Related Documents** 11

1. PURPOSE

The purpose of this policy is to provide direction and support to ensure the protection of 'Privi Speciality Chemicals Limited' hereafter referred to as 'PSCL' to allow access, use, and disclosure of PSCL managed systems in accordance with relevant business requirements and defined policies.

2. OBJECTIVES

- The varied challenges presented by cyber risk should be met with a broad response.
- To provide guidelines for addressing cyber security and related risks and the mitigation of such risks.
- Appropriately - management's attention is a necessity, as is an effective governance structure able to identify, protect, detect, respond to, recover from, test, learn, and be aware of cybersecurity incidents.
- To prevent the occurrence and recurrence of cyber incidents by implementing security proactive/ protective measures.
- To create infrastructure for conformity assessment with cybersecurity best practices, standards, and guidelines
- To create processes, structures, and mechanisms to generate necessary situational scenarios of existing and potential cybersecurity threats and enable timely information sharing for proactive, preventive, and protective actions.
- To promote and launch a comprehensive awareness program on information and cybersecurity.

- To protect and guard the PSCL IT infrastructure from cyber threats.

3. SCOPE

The policy applies to - PSCL users who have access to PSCL Managed systems and are required to comply with all policies referred to in this document.

The policy applies to all the offices and employees of the PSCL within India.

This policy also extends to all affiliates and subsidiaries of PSCL subject to adoption by the Board of the respective affiliate and subsidiary company.

4. ROLES AND RESPONSIBILITIES

The Cyber Security Policy has been issued under the authority of the IT Head and is owned and governed by the IT Team.

The IT Team under the direction of the IT Head is responsible for reviewing/updating and monitoring compliance with the policy.

5. POLICY STATEMENT

5.1. CYBER RESILIENCE PROGRAM

- Cyber resilience is the ability to continuously deliver the intended outcome despite adverse cyber events. Well-functioning cybersecurity management program consistent with cyber resilience best practices shall be in place and verified through supervisory review.
- Best practices for cyber resilience should include but not be limited to the below key areas:

  Identification: critical IT assets and risks associated with such assets.

Protection: assets by deploying suitable controls, tools, and measures.

Detection: incidents, anomalies, and attacks through appropriate monitoring tools/processes.

Response and Recovery: by taking immediate steps after identification of the incident, anomaly, or attack and 'recovering' from the incident as defined in the *POL-IT-008 Incident Management Policy*.

Identification

- The following cyber threats shall be identified (Threat Catalogue *'ASD-IT-003-2'*):
  - That could affect the operational performance
  - Cause significant impact to meet "PSCL" business objectives and obligations
  - Cause threat to critical business, processes, and reputation
- Necessary steps shall be taken to identify assets that need to be protected on priority.
  - Critical assets shall be identified that shall be protected against compromise *'ASD-IT-002-1'*.
  - PSCL managed systems (including sensitive personal information) and related system access shall be part of the identification process.
  - Business process or vendor risk shall be identified and assessed as a part of the on-boarding and operations process.
  - Critical Systems and Cyber Security incidents shall be classified based on criticality and severity as defined in *SOP-IT-002 Security Categorization of*

PSCL Information and Information System Procedure and *POL-IT-008 Incident Management Policy.*

- Testing programs, vulnerability assessments, and penetration tests are the cornerstones in the testing phase.

Protection

- Security controls shall be in line with technical standards. Resilience shall be provided by design. Comprehensive protection involves protecting inter-connections and other means of access to insider and outsider threats. When designing protection, the "human factor" shall be taken into consideration.
- Appropriate access controls on least privileged roles shall be part of the application and access control design.

Detection

- For critical systems, cybersecurity monitoring is essential as performing security events monitoring and or analytics shall assist in the detection and mitigation of cyber incidents. These shall include third-party providers also.

Response and Recovery

- It is not always possible to detect or prevent cyber incidents before they happen even with the best processes in place. For this reason, incident response planning is of great importance. Resumption of services (if interrupted) shall be achieved within a reasonable time frame depending on the impact of the incidents and the criticality of the service.

- Contingency planning, design, and business integration as well as data integrity (also in the case of data sharing agreements) are key enablers for fast resumption.
- For effective contingency planning, regular testing shall be conducted at regular intervals. Forensic readiness shall be facilitated for the investigations if needed.

Learning and Reporting

- PSCL shall continually re-evaluate the effectiveness of cybersecurity management. Lessons learned from cyber events and cyber incidents contribute to improved planning. New developments in technology shall be monitored and include necessary actions in the continual program.
- Cybersecurity incidents that are critically affecting the business operations and a large number of customers shall be reported to the respective department head.

Training

- It is mandated that periodic training programs be conducted to enhance the awareness levels among PSCL Users regarding information security at least annually. These training programs are designed to ensure that PSCL Users possess the requisite knowledge and skills to effectively safeguard sensitive information and mitigate potential risks.

- These training programs will cover a wide range of topics, including but not limited to:

- Best practices for handling and protecting sensitive information.
- Identification and mitigation of potential risks and threats.
- Compliance with relevant laws, regulations, and industry standards.
- Incident response procedures and protocols.
- Emerging trends and technologies in information security.

- It is the responsibility of all PSCL Users to actively participate in these training programs as mandated by the policy. By complying with this requirement, PSCL Users demonstrate their commitment to upholding information security standards and mitigating risks to the organization.

- Furthermore, PSCL will maintain records of the training sessions conducted, including participant attendance as evidence of compliance with this policy. These records will be periodically reviewed to ensure adherence to the training program and to identify areas for improvement.

5.2. POLICY COMPLIANCE

- Failure to comply with this policy shall result in disciplinary action.
- Respective department heads and IT Team shall ensure adherence to this policy and shall be responsible for appropriate remedial action.
- In case of any exceptions to this policy, exception approval needs to be taken which includes providing a valid business justification, risk acceptance from department heads, and approvals from IT Head.

6. ACTIVITIES/RECORDS TO BE MAINTAINED

Sr. No.	Name	Type	Record Number	Frequency	Responsibility
1	List of Critical IT assets along with associated Risk	Record	ASD-IT-002-1	On-going	IT Team
2	Threat Catalogue	Catalogue	ASD-IT-003-2	On-going	IT Team
3	Training sessions	Record	NA	Annual	IT Team

7. Related Documents

- POL-IT-001 IT Governance
- POL-IT-002 Information Security Policy
- POL-IT-008 Incident Management Policy
- POL-IT-010 Email Security Policy
- POL-IT-011 Endpoint Security Policy
- POL-IT-014 Physical Security Policy
- SOP-IT-002 Security Categorization of PSCL Information and Information System Procedure
- SOP-IT-003 Information Security Risk Management Procedure