Cohance

INFORMATION SECURITY MANAGEMENT SYSTEM

INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

VERSION 1.1

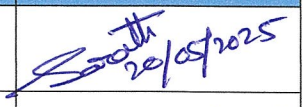
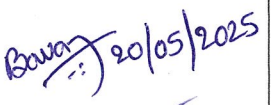
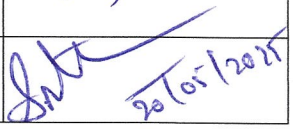
20TH MAY 2025

DOCUMENT CONTROL

Document Information

Document No.	Title	Version No.	Description
Cohance-ISMS-PY-08	Information Security Incident Management Policy	1.1	This document provides policy direction for information security incident management in Cohance.

Responsibilities

	Name	Role	Sign & Date
Prepared by	Sarath Kumar Reddy Gaddam	Sr. Manager, IDS	
Reviewed & approved by	Pavan Boddapati	Information Security Manager	
Authorized by	Nitin Kumar Shantha	Chief Information Officer	

Version History

Version No.	Release Date	Prepared by	Reviewed By	Version Description
1.0	25th June 2024	Sarath Kumar Reddy Gaddam	Pavan Boddapati	First Release
1.1	20th May 2025	Sarath Kumar Reddy Gaddam	Pavan Boddapati	Logo Changed, Second Release

Contents

1. INTRODUCTION

Cohance Lifesciences Limited (hereafter referred to as "Cohance") is a leading CDMO and API platform, offering products and services across all phases of a molecule's lifecycle adhering to the highest standards of Safety and Quality. Cohance is committed to protecting its customers, employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly when using Cohance digital assets. In the era of digital transformation and ever evolving threat landscape, security incidents, breaches and loss of data are a reality for many organizations. This Information Security Incident Management Policy together with the high-level Information Security Policy and other topic specific policies provide the required policy direction and mandates as well as guidelines for information security within **Cohance**.

2. OBJECTIVE

The objective of this Policy is to define the rules of Information Security Incident Management process for effectively responding to incidents and restoring services as soon as possible, and communicating the resolution to the end user.

3. SCOPE

This Policy applies to all digital assets of Cohance as well as employees and contractors of Cohance and third-party personnel using Cohance digital assets.

4. POLICY

4.1 Responsibilities and Procedures

4.1.1 The CIO as Head of Information Security function shall be responsible for managing the information security incidents and coordinating related actions.

4.1.2 Cohance shall plan and prepare for its response to information security incidents by defining, establishing, and communicating information security incident management procedures, roles and responsibilities.

4.2 Logging and monitoring

4.2.1 Logs that record activities, exceptions, faults, and other relevant information security events shall be defined, produced, stored, protected, and analysed.

4.2.2 An audit trail of system access and data use shall be maintained wherever practical and reviewed regularly.

4.2.3 The activity of all accounts shall be monitored to identify any abuse of access or compromise of the account.

4.2.4 Networks, systems, and applications shall be monitored for anomalous behaviour and appropriate actions shall be taken to evaluate potential information security incidents.

4.3 Reporting Information Security Events

4.3.1 Information Security events / incidents shall be reported from all relevant sources, including users, audit process, ISOC, advisory team, customers, etc.

4.3.2 Employees, contractors and third party users of information systems and services shall note and report any observed or suspected security weakness in the company's systems or services before it leads to an incident or violation.

4.3.3 Employees, contractors and third party users shall report violations, incidents and security weaknesses to the Helpdesk or the ISM.

4.3.4 For critical incidents that need communication to be sent out to employees, regulators or customers, timely breach notification shall be sent out as per the contractual or regulatory requirement.

4.3.5 Appropriate trainings shall be provided to all the users to create awareness on incident reporting procedures; and to the technical teams with the responsibilities for addressing security breaches on incident response.

4.4 Assessment of and Decision on Reported Information Security Events

4.4.1 All incidents reported (hereafter violations and security weaknesses shall be included and referred as incidents) shall be logged with all relevant details in a centralized system and tracked to closure.

4.4.2 Incidents logged shall have a unique identifier as per the agreed standard nomenclature.

4.4.3 All Incidents logged shall be assessed for the business impact in order to determine the best course of action to take. Based on the assessment, the incidents shall be categorized as per the defined Incident Management Matrix. *[Refer Incident Management Procedure for the Matrix].*

4.4.4 Incidents whose resolution may require a change shall be governed by the Change Management Policy and Procedure.

4.4.5 Cohance shall review and update, if required, the incident classification criteria on an annual basis.

4.5 Incident Response

4.5.1 The information security incident management procedures defined shall ensure that:

a) All incidents logged shall be assigned to respective support functions for analysis and resolution.

b) All emergency actions taken shall be documented in detail.

c) Emergency action shall be reported to management and reviewed.

d) The integrity of business systems and controls shall be confirmed with minimal delay.

4.5.2 The Incident Response Procedures that shall be integrated with **Cohance's** crisis management plan and business continuity plan.

4.5.3 The incident response team shall identify incident response actions and assign them to responsible parties. They shall ensure that all reported security incidents are responded and resolved timely, and if not, then escalated as per the classification of security incidents.

4.5.4 The Information Security Function shall periodically test and refine information security incident response procedures based on test results, lessons learned from previous incidents and to incorporate industry development.

4.5.5 Audit trails and similar evidence shall be collected and secured, as appropriate, for:

- Internal problem analysis later.
- Use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings e.g. under Copyrights Act, Information Technology Act 2000, GDPR or the Digital Personal Data Protection Act, 2023.
- Negotiating for compensation from software and service suppliers.
- Settlement of Insurance claims, wherever applicable.

4.5.6 Root Cause Analysis (RCA) shall be conducted for all major incidents as determined by the Information Security Manager.

4.5.7 Disciplinary actions shall be determined based on the Incidents severity and RCA report by a committee of relevant stakeholders set up by the CIO.

4.5.8 CIO shall be responsible to approve the punitive actions in consultation with Human Resource team for incidents with "high" severity.

4.5.9 Corrective actions recommended in the Root Cause Analysis and Corrective Action Report shall be performed in a timely manner.

4.5.10 All logged incidents shall be assigned to respective support groups for resolution.

4.5.11 All incidents shall be resolved in accordance with the defined SLAs.

4.6 Incident Communications

4.6.1 When a major information security incident is detected at **Cohance**, the CIO shall send out appropriate communication to regulatory authorities and relevant customers as per the timelines agreed in the Contracts.

4.6.2 Incidents status shall be tracked and communicated to the affected stakeholders throughout the lifecycle of the incident.

4.6.3 Appropriate control shall be followed to prevent unauthorized release of information during the course of incident or investigation.

4.6.4 Any release of information shall be authorized by the Corporate Communications.

4.7 Collection of Evidence

4.7.1 Controls shall be defined and applied for the identification, collection, acquisition and preservation of information, which can be used as evidence, especially if criminal or civil proceedings likely to happen from the incident.

4.7.2 The ISM shall ensure that all relevant evidence is collected for conducting necessary investigation, and the event logs shall be retained for a time period as required by legal, regulatory or other compliance obligations.

4.8 Forensic Investigation

4.8.1 The Information Security function shall perform digital forensic investigations for incidents requiring forensic investigation for legal or regulatory purposes or contractual obligations and /or severe information security incidents.

4.8.2 The Information Security function shall perform due diligence on technical sources, consultancy firms or forensic service firms before engaging for forensic investigation.

4.8.3 The Information Security function shall collect, process, store and analyze digital evidence in accordance with the regulations and laws that are applicable to **Cohance** environment in the relevant jurisdiction(s) for any security incidents where forensics evidence is required.

4.9 Incident Closure

4.9.1 Incidents closure shall be based on the confirmation received. Documentary evidence shall be maintained for the confirmation.

7. ABBREVIATIONS AND TERMS

Acronym / Term	Definition
CIO	Chief Information Officer
GDPR	The General Data Protection Regulation
ISOC	Intelligent Security Operations Centre
ISM	Information Security Manager
ISMS	Information Security Management System
RCA	Root Cause Analysis
SLA	Service Level Agreement

***