Cohance

INFORMATION SECURITY MANAGEMENT SYSTEM

DATA LEAK PREVENTION POLICY

Version 1.1

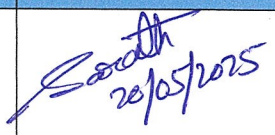
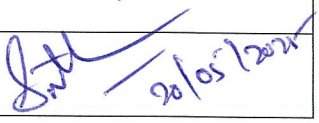
MAY 20, 2025

DOCUMENT CONTROL

Document Information

Document No.	Title	Version No.	Description
Cohance-ISMS-PY-07	Data Leakage Prevention Policy	1.1	This document provides policy direction to stop the exfiltration of data and intellectual property to prevent unintentional leaks or data breaches.

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 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. Data leakage is a common problem within organisations that deal with large amounts of data, of different classifications, across multiple standalone and linked ICT systems, applications and file servers. This Data Leakage Prevention (DLP) Policy provides policy direction and security strategy that safeguards sensitive data by identifying, monitoring, and protecting it.

2. OBJECTIVE

The objective Policy is to ensure that sensitive information, such as customer information, financial data, and intellectual property is protected, and data breaches are to be prevented.

3. SCOPE

This Policy applies to IT resources in use in Cohance and all employees and contractors, and 3rd party software service providers.

4. POLICY

4.1 Data leakage prevention

4.1.1 Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.

4.2 Data Discovery and Classification

4.2.1 The type of data Cohance has, where it's stored, and who has access to it shall be identified.

4.2.2 The data shall be classified based on its sensitivity and importance and in accordance with Cohance's Information Classification Scheme.

4.3 Implementation of Data Loss Prevention Tools

4.3.1 Appropriate DLP tools shall be deployed to configure and enforce policies to prevent unauthorized access, usage, or transfer of sensitive data; and receive alerts on potential threats and gain visibility into data activity.

4.4 Endpoint Security

4.4.1 All endpoint devices processing, storing and transmitting sensitive corporate information shall be identified and centrally authenticated through Domain Controller. Exceptions to this shall be recorded and approved.

4.4.2 All endpoints shall be uniquely identified and labelled using a unique and standardized nomenclature.

4.4.3 Endpoint security shall be deployed to prevent endpoint devices from becoming vulnerable to cyber-attacks and protect Cohance's data.

4.4.4 All endpoint devices shall be configured as per the Minimum Baseline Security Standard (MBSS).

4.4.5 Restricted services and processes shall be configured on all endpoint devices.

4.4.6 Administrative access to endpoint devices shall be restricted to a few appropriate individuals.

4.4.7 Network traffic filtering on endpoint devices shall be implemented.

4.4.8 Restricted internet access shall be configured on all endpoint devices. Exceptions to this shall be recorded and approved.

4.4.9 All endpoint capable of running host firewall software shall do so to protect the device from external threats such as hacking by unauthorized parties.

4.4.10 Endpoints storing sensitive or confidential data shall have appropriate security controls and encryption standards necessary for their protection.

4.5 Monitoring Data Activity

4.5.1 Data activity shall be regularly monitored real-time to detect unauthorized access or usage and enable timely action.

4.6 Review and Update of Policies

4.6.1 The DLP policies shall be regularly reviewed to ensure they remain effective against new threats and changes in the Cohance's data environment and to reflect changes in the Cohance's data classification, access controls, monitoring, employee education, encryption, and backup plans.

4.7 Employee Education

4.7.1 Regular training for employees and contractors shall be conducted on data security best practices, such as password management, email security, safe browsing, data privacy.

5. POLICY COMPLIANCE

5.1 Compliance Checks

Compliance with this Policy is mandatory. The Cyber Security or HR Manager shall verify compliance to this policy through various methods, including but not limited to, security monitoring, business tool reports, internal and external audits, and provide feedback to the Leadership team / Policy Owner.

5.2 Review

This Policy shall be reviewed every two years or whenever there are technology / business changes impacting the policy implementation.

5.3 Exceptions

Any exception to this policy must be approved in writing by the Policy Owner in advance.

5.4 Non-Compliance

An employee / contractor found to have violated this policy may be subject to disciplinary action, up to and including termination of employment / contract.

6. RELATED PROCEDURES

The following procedures assist in implementing this Policy:

S.No.	Name of the Related Procedure	Reference Section
1.	IT Roles and Responsibilities	Entire document
2.	Incident Management Procedures	Entire document

7. ABBREVIATIONS AND TERMS

Acronym / Term	Definition
DLP	Data Leakage Prevention
MBSS	Minimum Baseline Security Standard

NDA	Non-Disclosure Agreement

***