Cohance

**INFORMATION SECURITY MANAGEMENT SYSTEM**

# PHYSICAL & ENVIRONMENTAL SECURITY POLICY

Version 1.1

MAY 20, 2025

# DOCUMENT CONTROL

## Document Information

| Document No. | Title | Version No. | Description |
|---|---|---|---|
| Cohance-ISMS-PY-11 | Physical & Environmental Security Policy | 1.1 | This document provides policy direction for employees and contractors to ensure protecting ICT equipment and supporting utilities. |

## Responsibilities

| | Name | Role | Sign & Date |
|---|---|---|---|
| Prepared by | Sarath Kumar Reddy Gaddam | Sr. Manager, IDS | Sarath 20/05/2025 |
| Reviewed & approved by | Pavan Boddapati | Information Security Manager | Pavan 20/05/2025 |
| Authorized by | Nitin Kumar Shantha | Chief Information Officer | 20/05/2025 |

## Version History

| Version No. | Release Date | Prepared by | Reviewed By | Version Description |
|---|---|---|---|---|
| 1.0 | 27th June 2024 | Sarath Kumar Reddy Gaddam | Pavan Boddapati | First Release |
| 1.1 | 20th June 2024 | 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. Physical security is a critical part of Cohance's security program. It forms the basis for all other security efforts, including personal and information security. This Physical & Environmental Security Policy provides policy direction to ensure protection of Cohance's information, information resources and human assets.

# 2. OBJECTIVE

The objective Policy is to prevent unauthorised physical access, damage and interference to the organisation's information, information processing facilities and human assets.

# 3. SCOPE

This Policy applies to all employees, contractors, visitors, information and information processing facilities.

# 4. POLICY

## 4.1 Physical Security Perimeters

4.1.1 Security perimeters and boundaries shall be defined and used to protect areas that contain information and any information processing assets / facilities.

4.1.2 Areas containing key IT infrastructure equipment (Server Rooms, DC etc.) shall have additional physical security barriers to provide additional protection to those assets.

## 4.2 Physical Entry

4.2.1 Secure areas shall be protected by the appropriate entry controls to ensure only authorised personnel are allowed access.

4.2.2 Access points such as delivery and loading areas and other points where unauthorized persons can enter the premises shall be controlled, and if feasible, isolated from information processing facilities to avoid unauthorized access.

4.2.3 A physical logbook or electronic audit trail of all access shall be securely maintained and monitored.

4.2.4 All logs and sensitive authentication information shall be appropriately protected.

## 4.3 Securing Offices, Rooms and Facilities

4.3.1 Appropriate physical security for offices, rooms and facilities shall be designed and implemented.

## 4.4 Physical Security Monitoring

4.4.1 Physical Premises shall be continuously monitored by surveillance systems to detect and deter unauthorized physical access.

4.4.2 Monitoring systems shall be protected from unauthorized access in order to prevent surveillance information, such as video feeds, from being accessed by unauthorized persons or systems being disabled remotely.

4.4.3 Any monitoring and recording mechanism used shall take into consideration local laws and regulations including data protection and PII protection legislation, especially regarding the monitoring of personnel and recorded video retention periods.

## 4.5 Protecting against External & Environmental Threats

4.5.1 Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed based on risk assessment results and implemented.

## 4.6 Working in Secure Areas

4.6.1 Security measures covering all activities taking place in the secure areas shall be designed and implemented.

## 4.7 Equipment siting and Protection

4.7.1 Equipment shall be sited securely and protected to reduce the risks from environmental threats and hazards, and against unauthorised access.

## 4.8 Security of Assets off-Premises

4.8.1 Devices which store or process information outside the organization's premises shall be protected appropriately.

## 4.9 Storage Media

4.9.1 Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the Cohance's classification scheme and handling requirements.

4.9.2 Appropriate procedures for the secure reuse or disposal of storage media shall be established to minimize the risk of unauthorized disclosure of confidential information.

## 4.10 Supporting Utilities

4.10.1 Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.

## 4.11 Cabling Security

4.11.1 Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.

## 4.12 Equipment Maintenance

4.12.1 Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information

## 4.13 Secure disposal or re-use of equipment

4.13.1 Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

# 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 |
|---|---|
| DC | Data Centre |
| ISO | International Standards Organization |
| NDA | Non-Disclosure Agreement |

***