Cohance

INFORMATION SECURITY MANAGEMENT SYSTEM

SUPPLIER SECURITY POLICY

Version 1.1

JUNE 17, 2025

Cohance Confidential

DOCUMENT CONTROL

Document Information

Document No.	Title	Version No.	Description
Cohance-ISMS-PY-27	Supplier Security Policy	1.1	This document outlines the principles, guidelines, and best practices to ensure information security in supplier relations.

Responsibilities

	Name	Role	Sign & Date
Prepared by	Sarath Kumar Reddy Gaddam	Sr. Manager, IDS	Sarath 17/06/25
Reviewed & approved by	Pavan Boddapati	Information Security Manager	17/06/25
Authorized by	Nitin Kumar Shantha	Chief Information Officer	17/06/25

Version History

Version No.	Release Date	Prepared by	Reviewed By	Version Description
1.0	30th July 2024	Sarath Kumar Reddy Gaddam	Pavan Boddapati	First Release
1.1	17th June 2025	Sarath Kumar Reddy Gaddam	Pavan Boddapati	Logo changed, Second Release

Contents

1. INTRODUCTION

External suppliers are a necessary component of any business operations, especially in pharma sector. These suppliers may have access to a wide range of information of the organizations they support. Therefore, it is crucial for the operation and effectiveness of Cohance's Information Security Management System that its relationships with suppliers are based on a clear understanding of each party's expectations and requirements around information security. This document specifies rules and standards to address supply chain security risks.

2. OBJECTIVE

The objective of this policy is to establish rules for maintaining agreed level of information security in supplier relationships.

3. SCOPE

This policy applies to all Cohance employees, contractors, its third-party service providers as well as Cohance information and information resources.

4. POLICY

4.1 Choosing a Supplier

4.1.1 For effective management of supplier relationships, a risk-based approach shall be taken. Suppliers shall be classified into the following three categories based on their impact on the confidentiality, integrity, and availability of Cohance information, their value and risk to Cohance operations:

i. **Class A:** Critical Vendor with high information security risk
ii. **Class B:** Important Vendor with medium information security risk
iii. **Class C:** Transactional Vendor with low information security risk

4.1.2 A centralised inventory of suppliers shall be maintained. It shall list type of supplier (such as ICT Services, Logistics, Utilities, Financial Services, ICT Infrastructure components) supplier contact details and other essential information to effectively manage the relationship.

4.1.3 Appropriate due diligence and risk assessments shall be carried out in selecting and approving new suppliers before contracts are agreed upon.

4.1.4 Processes and criteria shall be established for regular (at least annual) performance monitoring and risk assessment of the supply chain relationships.

4.1.5 Cohance risk management process (refer to Information Security Risk Management Methodology) shall consider the risks associated with:

a) the suppliers' use of Cohance information and other associated assets, including risks originating from potential malicious supplier personnel

b) malfunctioning or vulnerabilities of the products (including software components and subcomponents used in these products) or services provided by the suppliers

4.1.6 Close contact shall be maintained with the cloud service providers to enable a mutual exchange of security information for the use of the cloud services.

4.2 Supply Chain Risk Management

4.2.1 The third party risk identification and risk mitigation for the three classes of vendors shall be addressed as per the Third Party Risk Strategy described in Annexure A: Third Party Risk Strategy.

4.2.2 Third party vendors handling any of Cohance's sensitive information shall agree to sign off Confidential Disclosure Agreement (CDA). The CDAs shall be signed off between all Class A, B and C third party vendors and respective business teams.

4.2.3 Prior to third party vendor empanelment, an initial Due Diligence shall be performed by Cohance to identify any risks that may be non-compliant with Cohance's information security requirements. The Due Diligence activity shall also allow third party vendors and Cohance business teams to implement mitigating controls against the non-compliances identified prior to third party vendor empanelment.

4.2.4 Third Party vendors shall be included as part of Vendor Risk Assessments.

4.2.5 The type of audits to be performed for the third party vendors shall be Onsite Audits (full scope), Desktop Audits and Self-Assessment. The assignment of the audits shall be as follows:

- Onsite Audits – for Class A Vendors
- Desktop Audits – for Class B Vendors
- Self-assessments – for Class C Vendors

4.2.6 Onsite Audits

4.2.6.1 On-site third party vendor audits shall be performed for Critical Vendors with high information security risk, that is, Class A Vendors.

4.2.6.2 On-site audits would comprise of site audits by performing physical verification of the information security controls.

4.2.6.3 The scope of the audit shall be discussed and agreed between Cohance and Class A third party vendor.

4.2.6.4 Audit findings shall be documented, validated and agreed with the third party vendors.

4.2.6.5 Cohance ISM shall ensure that the Third party vendors take necessary action to close the audit findings.

4.2.7 Desktop Audits

4.2.7.1 Desktop Audits shall be conducted for Class B Vendors remotely from Cohance's premises. It shall involve the review of evidence provided to meet Cohance's Information Security controls.

4.2.7.2 The third party vendor shall ensure that there are adequate provisions for the logging of events on the service to record the following at a minimum:

- Legitimate access
- Authentication exceptions
- Authorisation exceptions
- Privilege changes
- Data object owner changes
- Export of information
- Out of hours access

4.2.7.3 The third party vendor shall ensure that audit trails are regularly and effectively inspected for information security incidents.

4.2.7.4 The third party vendor shall have processes and procedures in place to manage the investigation and closure of security incidents.

4.2.8 Self-assessments

4.2.8.1 Self-assessment shall be conducted for Class C Vendors. It involves assessing the vendor's responses to Cohance's Information security controls questionnaire. Following areas, at a minimum, shall be covered in the self-assessment questionnaire:

- IS policies and procedures
- Data security and privacy
- Human Resource Security
- Change and patch management
- Logical access management
- Remote access and VPN
- Network infrastructure security
- Physical and environmental security
- Backup and restoration
- Disaster recovery and business continuity planning
- Information security awareness
- Compliance

4.2.8.2 Risk areas shall be identified based on the responses received from the third party vendors.

4.2.8.3 Cohance ISM shall ensure that the third party vendors take necessary actions to mitigate the identified risks.

4.2.9 Ad-hoc audits shall be carried out, where necessary, for all Class A, B and C third party vendors so as to meet Cohance's internal compliance and/ or Information security requirements.

4.3 Agreements with Suppliers

4.3.1 All third party vendors shall sign a Confidentiality Disclosure Agreement (CDA) prior to being given access to Cohance's information and information systems.

4.3.2 Relevant information security requirements and controls must be formally documented in a contractual agreement that may be part of, or an addendum to, the main commercial contract with the suppliers. The key information security requirements that shall be considered include:

4.3.2.1 Both parties' rights categorised into four main areas – legal, statutory, regulatory and contractual. Within these four areas, various obligations should be clearly outlined, as is standard in commercial agreements, including accessing PII, intellectual property rights and copyright stipulations. The agreement should also cover how each of these key areas will be addressed in turn.

4.3.2.2 A clear understanding of what constitutes both acceptable and unacceptable use of information, and physical and virtual assets from either party.

4.3.2.3 Procedures that deal with the levels of authorisation required for supplier-side personnel to access or view an organisation's information (e.g. authorised user lists, supplier-side audits, server access controls).

4.3.2.4 Courses of action open to the organisation in the event of a breach of contract on the part of the supplier, or failure to comply with individual stipulations.

4.3.2.5 A mutual Incident Management procedure that clearly stipulates what needs to happen when problems arise, particularly concerning how the incident is communicated between both parties.

4.3.2.6 Personnel from both parties should be given adequate awareness training (where standard training is not sufficient) on key areas of the agreement, specifically concerning key risk areas such as Incident Management and the provision of access to information.

4.3.2.7 Adequate attention should be given to the use of subcontractors. If the supplier is permitted to use subcontractors, the organisations should take steps to ensure that any such individuals or companies are aligned with the same set of information security requirements as the supplier.

4.3.2.8 The agreement should take steps to ensure the timely and thorough resolution of any defects or conflicts that take place during the course of the relationship.

4.3.3 Separate non-disclosure agreements shall be used where a more specific level of control over confidentiality is required, or information is shared before the finalisation of commercial contracts. Additional security vetting may be necessary for accessing client information.

4.3.4 The supplier shall ensure its supply chain, including sub-contractors, who play a part in the delivery of goods or services to Cohance, comply with the information security requirements agreed within the agreements.

4.3.5 The agreements with suppliers shall be regularly reviewed and validated to ensure they are still fit for purpose.

4.4 Additional Rules applicable to the ICT Supply Chain and Critical Suppliers

4.4.1 The information security controls in place at existing suppliers (where due diligence was not undertaken as part of the initial selection) shall be clearly understood and improved where necessary.

4.4.2 Business continuity and assurances for continuing service delivery in the event of a supplier failure or disaster shall be addressed.

4.4.3 Within supplier inventory, the following shall be noted and kept up to date:

a) lead contact name and contact details
b) where necessary, escalation paths.
c) Contact details of the supplier's Data Protection Officer

4.4.4 Where deemed necessary by risk assessment, the following details shall be obtained from the critical suppliers during onboarding and regular reviews:

a) critical components and dependencies within their supply chain
b) necessary assurance that the products and services in question have achieved the required security levels
c) awareness and training requirements for both parties to the agreement, based on the terms of the agreement and defined processes

4.5 Cloud Services

4.5.1 Cohance information shall only be stored within cloud services after a risk assessment has been performed. The risk assessment process shall involve a complete understanding of the information security controls implemented by the cloud service provider.

4.5.2 The use of cloud services involves shared responsibility for information security. The responsibilities of the cloud service provider and Cohance, acting as the cloud service customer, for each CCM (Cloud Controls Matrix) domain defined by Cloud Security Alliance (CSA) shall be defined using a shared security responsibility matrix for each critical cloud service and implemented appropriately.

4.6 Managing Changes to Supplier Services

4.6.1 Changes to services provided by suppliers shall follow the change management process, where applicable, to assess any information security implications of changes so that the effectiveness of controls is maintained.

4.6.2 The end of contract terms shall clearly outline the requirements to ensure secure termination of the supplier relationship, including:

i. de-provisioning of access rights,
ii. information handling,
iii. determining ownership of intellectual property developed during the engagement,

iv. information portability in case of change of supplier or insourcing,
v. records management
vi. return of assets,
vii. secure disposal of information and other associated assets, and
viii. ongoing confidentiality requirements

4.6.3 The end of the contract shall be requested in writing within the agreed terms.

4.6.4 Transfer of supplier services from the incumbent to another party shall be planned as a project, and appropriate change control procedures shall be followed.

4.7 Monitoring and Review of Supplier Services

4.7.1 The service reports produced by the supplier shall be reviewed and regular progress review meetings shall be arranged as required by the agreements.

4.7.2 Audit of suppliers and sub-suppliers, in conjunction with review of independent auditor's reports, if available shall be conducted and follow-up action shall be taken on issues identified.

4.7.3 A thorough record of information security events, tangible operational problems, fault logs and general barriers to the service delivery standards that have been agreed shall be maintained and reviewed.

4.7.4 Any identified information security events or incidents shall be responded to and take managed

4.7.5 Any information security vulnerabilities shall be identified and remediated.

4.7.6 Any relevant information security factors inherent within the supplier's relationship with its own suppliers and subcontractors shall be reviewed.

4.7.7 It shall be ensured that the supplier maintains sufficient service delivery capability together with workable plans designed to ensure that agreed service continuity levels are maintained following service failures or disaster.

4.7.8 It shall be ensured that the supplier assigns responsibility to key personnel in the supplier's operation who are responsible for maintaining compliance and enforcing the requirements of the agreements.

4.7.9 Regular evaluations shall be conducted to ensure that the suppliers maintain adequate information security levels. (Refer section 4.2 Supplier Risk Management)

4.7.10 The results of the reviews and audits shall be communicated to the senior management.

5. POLICY COMPLIANCE

5.1 Compliance Checks

Compliance with this Policy is mandatory. The Information Security 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.	EU-GMP Annex 11, US-FDA CFR-21	Entire document

7. ABBREVIATIONS AND TERMS

Acronym / Term	Definition
CCM	Cloud Controls Matrix
CDA	Confidentiality Disclosure Agreement
CSA	Cloud Service Agreement
CSP	Cloud service providers
DR	Disaster Recovery
ICT	Information and Communication Technology
NDA	Non-Disclosure Agreement

PII	Personal Identifiable Information
SLA	Service Level Agreement

8. ANNEXURE-A: THIRD PARTY INFORMATION SECURITY RISK STRATEGY

8.1 Third Party Risk Strategy

Vendor Classification **Strategy Elements**	**Class A**	**Class B**	**Class C**
Classification	Critical Vendor with high information security risk	Important Vendor with medium information security risk	Transactional Vendor with low information security risk
Contract / Agreement	Yes	Yes	Yes
Confidential Disclosure Agreement (CDA)	Yes	Yes	Yes
Initial Due Diligence	Yes	Yes	Yes
Vendor Risk Assessment	Yes	Yes	Yes
Audit Type	Onsite audit	Desktop audit	Self-Assessment
Audit Cycle	Yearly	Yearly	Yearly
Ad-hoc audits	Yes	Yes	Yes

8.2 Vendor Governance Calendar

Vendor Classification	**Initial Due Diligence**	**Performance Review Meetings Frequency**	**Audit Scope**	**Audit Cycle**
Class A	• Required	• Quarterly	On-site audit (full scope)	Annual
Class B	• Required	• Annual	Desktop audit	Annual
Class C	• Required	• Annual	Self-assessment	Annual

***