This document is applicable when in Effective status

Effective Date (GMT) : 02 Oct 2025

Owning Department : Digital Digital CyberSecurity

Previous Document Number : STD-000395

Document Author Approval Task Approve	Leila BOUSFOUL, Cyber Security Expert Document Author Approval 01-Oct-2025 12:03:33 GMT+0000
Approval Task Approve	Jean-Yves POICHOTTE, Global Head of Cyber Security Risk & Compliance Approval 01-Oct-2025 13:13:20 GMT+0000
Approval Task Approve	Emilie DESCHAMPS, Risk Advisory Lead â€“ Cyber and Tech MS Quality Assurance Approval 02-Oct-2025 07:43:54 GMT+0000

Table of Contents

1. PURPOSE

This Standard describes the cybersecurity requirements applicable to Sanofi's Third-Parties / Contractors subject to the criteria defined in Section 2 below in order to mitigate the cybersecurity risks and protect Sanofi's assets.

2. SCOPE AND APPLICABILITY

These cybersecurity requirements are applicable to all Sanofi's Third-Parties / Contractors when at least one the following criteria is met:

- Third-Party / Contractor is handling Sanofi's Sensitive and/or Highly Sensitive Information or Personal Data (refer to *Information Classification Standard* : QU-STD-0000318);
- Third-Party / Contractor is supporting Sanofi business critical process(es) (i.e. importance to maintain Sanofi business continuity);
- Third party / Contractor has access to Sanofi's system/application (direct or interface). (i.e. means connection to Sanofi network and/or having credentials to Sanofi systems);
- Third party / Contractor is developing an AI* system for Sanofi or is using AI* to perform services and/or provide deliverables.

*AI means a digital artefact (business application, analytics dashboard, software as medical device, mobile application, etc.) that uses relevant data and AI learning techniques to generate insights for business use. The insights can be in the form of prediction, recommendation, new content, autonomous decision or manifest as automated actions.

3. REQUIREMENTS

This process is designed to ensure the effective management and mitigation of cybersecurity Third-party risks. Third-Party / Contractor must:

1) Demonstrate an acceptable maturity/ level of its information security program and service continuity via:
    - Cybersecurity recognized market certification covering the scope of services such as ISO27001 or SOC2 type 2 or Cybersecurity assessment performed by Sanofi validated partner
2) Commit to Cybersecurity measures by reviewing and adding to the contract the relevant contractual clauses using the Supporting Document Template (refer to QU-MT-0004647 *Third Parties / Contractors Cybersecurity Measures*).

If the Third-Party / Contractor does not demonstrate an acceptable maturity level or does not conform with any of the relevant cybersecurity requirements, the Requestor must

involve the Cybersecurity expert to review these documents and make recommendations to the project team.

4 RESPONSIBILITIES

It is the responsibility of the Global Head of Digital Cyber Security to design and monitor the application of this standard. The Requestor is responsible for the implementation and adherence to this process.

5 REFERENCES

Information Systems Security Framework Standard (QU-STD-0000126)

Information Classification Standard (QU-STD-0000318)

Third Parties / Contractors Cybersecurity Measures (QU-MT-0004647)

6 DEFINITIONS

Third-Party / Contractor: includes all entities with which Sanofi and/or Sanofi's affiliated companies have entered into a contract, regardless of the format (including purchase orders associated with Sanofi's general conditions of purchase). It includes partners, providers, suppliers, subcontractors, etc.

Requestor: the Sanofi employee who has initiated a request for a transaction in his/her scope of responsibility and is the owner of the transaction (e.g., end-user or any delegate thereof, including Procurement representative).

7 APPENDICES

Not Applicable

8 DOCUMENT HISTORY

Version Number	Version Application Date	Description of change
3.0	Refer to QualiPSO	**The main changes are:** Application of the Standard to Contractors using or deploying AI. Change the document reference for contractual measures: QU-MT-0004647-Third Parties / Contractors Cybersecurity Measures
2.0	31-May-2023	**The main changes are:** The scope and applicability have been revised to get Cybersecurity measures: - as a standalone document without quality part. - address all SANOFI Third Parties / Contractors All sections have been updated accordingly to answer to this new scope with a simplification approach . Renaming of the title of this STD-00395 by Third Parties / Contractors Cybersecurity requirements instead of Supplier Relationships
1.0	16-Jun-2022	This new Global Quality Standard, performed according to the new format, replaces the GDOPS-014311 - Supplier Relationships Operational Standard **The main changes are:** **Section 5** Updated document references to replace the following: - Information Security & Quality Legal/Contractual Guidelines for Cloud and/or Services Providers (GDSD-014400) with SD-000960, - Information Security & Quality Legal/Contractual Guidelines for License/Maintenance Providers (GDSD-014402) with SD-000961 - Information Security & Quality Legal/Contractual Guidelines for Shopfloor Providers (GDSD-014589) with SD-000962 - GDPOL-013876 with *Information Systems Security Framework* Standard (STD-000266) Changed ITS references to reflect Digital organization name throughout the document.

End of Document