Stellantis Global Supplier Information Security Requirements

Contents

Document History

Version	Month & Year	Comments	Owner
1.0	9 June 2022	Initial Document creation	Stellantis - Security Governance & Coordination Team

1. Introduction

The security requirements outlined herein are applicable to Third Parties that process, access, interact with, or store Stellantis data. This data may include intellectual property, customer or employee personal information, or other uncategorized Stellantis-owned data. In addition, this document applies to any Third Party that has access to Stellantis Information Systems through the Partner VPN or other approved method.

Stellantis reserves the right to update this document from time to time.

2. Purpose

The purpose of this document is to define the high-level security requirements Third Parties must follow to protect Stellantis information and IT (Information Technology) assets.

3. Applicability

These requirements apply to all Third Parties who:

1. Collect, transmit, manage, access, or store Stellantis Information (including intellectual property, customer/employee personal information, or other uncategorized Stellantis-owned data)
2. Provide Stellantis Vital or Critical Business Services
3. Connect to Stellantis Information Systems using the Partner VPN or other approved method.

4. Compliance

Third Party contracts in place prior to publishing of this document must minimally comply with the version of the Stellantis information security provisions or Third-Party Information Security Requirements specified in their contract and are subject to an annual request for attestation of compliance. Additionally, existing Third-Party agreements are subject to evaluation of inherent risk, based on the nature of the goods and/or services provided to Stellantis. Modifications to these Stellantis Third Party Information Security Requirements must be reviewed on a case-by-case basis.

5. Requirements

The following identifies the minimum level of Information Security Requirements:

#	Security Control		Requirements
1	Information Security Policy	1.1	Maintain an information security policy that, at a minimum, includes its overall objectives and scope and the importance of security to Third Party.
2	Password Controls And Access Management	2.1	Assign unique access/authentication credentials to each Third-Party Personnel with authorized access to Stellantis data.
		2.2	At a minimum comply with the password standards and requirements established by ISO 27002 or equivalent industry standard.
		2.3	Ensure segregation of duties through the use of role-based access controls.
		2.4	Promptly disable access privileges to Stellantis data for any Third-Party Personnel who are terminated or otherwise no longer need such access.
3	Encryption	3.1	Encrypt all Stellantis Data in transit and at rest using industry-standard encryption that meets NIST FIPS minimum requirements.
4	Anti-Malware Protection	4.1	Protect all IT systems from malware through the use of antivirus or other anti-malware practices
5	Network Security	5.1	Isolate trusted networks containing sensitive data from non-trusted networks.
		5.2	Encrypt wireless network traffic and implement default-deny, least-privilege policies on network firewalls.
6	Vulnerability Assessments	6.1	Implement a vulnerability assessment process that includes steps to prioritize high risk vulnerabilities and remediate identified security issues on infrastructure, middleware, and applications in a timely manner.
		6.2	Perform regular vulnerability scans and assessments to identify all potential vulnerabilities. Stellantis may ask for a vulnerability report for any systems that handle Stellantis data.
7	Incident Response	7.1	Have in place a security incident response plan for identifying, reporting, and appropriately responding to known or suspected security incidents impacting Stellantis data.
		7.2	Notify Stellantis of any security incidents impacting Stellantis Data or systems within 72 hours of detection and provide an action plan that includes coordination of investigation, impact to Stellantis data, and remediation activities.

8	System And Data Availability	8.1	Maintain an availability plan that can meet the business requirements outlined in the contractual agreements. This may include backups and restorations, disaster recovery, and business continuity for all locations and applications used to provide services to Stellantis.
		8.2	Maintain a business continuity plan for restoring normal business functions within the restoration requirements defined in the agreement.
9	Physical Security	9.1	Implement safeguards and controls that restrict unauthorized physical access to areas containing equipment used to access, store, or transmit Stellantis Data. This includes, but is not limited to access controls (keys, key cards, badge access, etc.), surveillance (Closed Circuity TV, networked security cameras, etc.), and alarms.
10	Data Retention And Destruction	10.1	At any time, and upon termination or expiration of business agreements, except to the extent required by law, immediately return or, if directed by Stellantis, securely destroy any and all Stellantis Data.
11	Subcontractors	11.1	Ensure Third Party workforce members working with Stellantis information are aware of and conform to these Third-Party Information Security Requirements as well as legal and regulatory requirements pertaining to Stellantis Information.
12	Security Awareness	12.1	Have a defined program to provide periodic information security awareness training to Third Party's workforce who will have access to Stellantis Data. Education and awareness training shall include the secure handling of Stellantis Data.
		12.2	Ensure all Workforce members are sufficiently educated to perform their jobs effectively and ensure the security of Stellantis Data.
13	Remote Access Control	13.1	Always use a Stellantis-approved method when connecting remotely.
		13.2	Provide Stellantis the right to monitor all network connections between Stellantis and Third Party.
14	Audit	14.1	Provide Stellantis, or a mutually agreed upon independent firm, permission to perform a security assessment to ensure compliance with the Third-Party Information Security Requirements and other contractual agreements.
15	Software Lifecycle	15.1	Information security checkpoints shall be incorporated into the software development lifecycle when necessary;

			a. Risk assessment process b. Documented security requirements c. Source code review d. Security testing e. Patch management f. Change management g. Problem Management
16	Communications	16.1	Stellantis Data must not be disclosed or communicated in any manner without approval in writing from Stellantis.
17	Configuration Management	17.1	Maintain a documented set of baseline security configuration standards for devices with the concept of Least Functionality.
		17.2	Monitor unauthorized changes or deviations from the Security Baselines in deployed devices.
18	Removable Media	18.1	Protect Stellantis data from unauthorized disclosure such as through the use of Data Loss Prevention Tools.
19	Security Assessment	19.1	Complete a Supplier Security Assessment within an agreed upon timeframe (typically 14 days after receipt of the assessment) if requested by Stellantis.

6. Definitions

Availability Plan	Plan to ensure availability requirements can be met as determined by the Agreement.
Agreement	The governing contracts, purchase orders, or other documented or non-verbal agreements between the Third Party and Stellantis that set forth the scope of products and/or services being provided.
Continuity Plan	Plan to quickly recover or ensure availability during unforeseen circumstances (i.e., natural disasters, power outages, pandemics, etc.).
Data Loss Prevention Tools	Information security tools that are used to prevent data loss by prohibiting the use of removable media, uploading data to unauthorized file sharing sites, or other industry standard data loss prevention strategies.
Third Party	Person, company, business, organization, vendors, contractor, sub-contractor, service provider, or other group that provides goods or services to Stellantis.
Security Baselines	Normal activity that is observed in everyday use of an Information System. Deviations from these baselines could be caused by a security incident.
Supplier Security Assessment	A self-attestation questionnaire that provides Stellantis with a overview of a supplier's internal information security practices. This questionnaire may be assigned to a supplier via a secured SaaS based platform.
Information System	Any electronic systems that handle information. This can include network infrastructure, servers, or other systems that support the terms outlined in the Agreement.
Least Functionality	Concept that ensures an Information System is configured only to provide the essential functionality and prohibits or significantly limits non-essential functions.
Partner VPN	A secured VPN that Stellantis provides to its suppliers when necessary. Access to the Partner VPN is provided on an as-needed basis.
Workforce	Employees, contractors, or other third parties that are supporting the Agreement.