Swegon

Sensitivity	Public
Owner	Head of Cybersecurity
Date	2026-11-18

Swegon Security Requirements for IT Service Providers

Information Security

2026-11-18 | Version 1.8



Table of Contents

1. Introduction 2
1.1. Purpose 2
1.2. Scope 2
2. Information Security Requirements 3
2.1. Regulatory Compliance 3
2.2. Security Framework 3
2.3. Roles and Responsibilities 3
2.4. Risk Management 3
2.5. Asset Management 3
2.6. Data Protection 3
2.7. Identity and Access Management 3
2.8. Logging and Monitoring 4
2.9. Security Validation 4
2.10. Lifecycle Management 4
2.11. Configuration Management 4
2.12. Incident Management 4
2.13. Change Management 4
2.14. Continuity Management 4
3. Exceptions 5
4. Related Resources 6
5. References 7
6. Document History 8

1. Introduction

1.1. Purpose

Swegon is committed to ensuring the availability, confidentiality, integrity and accountability of data, systems, and services.

This document establishes high-level minimum organisational information security requirements necessary to achieve and maintain these security properties in the use of third-party services.

The requirements are based on industry-standard frameworks, such as the ISO 27000-series and the NIST Cybersecurity Framework.

1.2. Scope

For the purposes of this document, service provider refers to an external party that delivers IT services to Swegon or that processes or has access to Swegon's information or systems, including vendors, suppliers, subcontractors, and third-party service providers.

These requirements apply to all products, components, and processes provided by the service provider that directly or indirectly support Swegon's assets and services, and extend to the service provider's subcontractors and third-party providers.

They apply to agreements entered into from the date of this version, shown on the cover, and to existing agreements at their renewal or amendment; Procurement carries them into the contract, as the Swegon Asset Management Guidelines describe.

This document does not cover the technical security requirements that apply per solution or product. Such requirements are laid out in Swegon Security Requirements for IT Solutions, Swegon Security Requirements for Products with Digital Elements (for products Swegon manufactures and places on the market), and Swegon Security Requirements for OT/ICS.

2. Information Security Requirements

The service provider shall comply with these requirements in a manner proportionate to its organisation, the type of products or services provided to Swegon, and the associated risks.

Exceptions to these requirements are handled as described in section 3.

The service provider shall, upon request, demonstrate compliance with these requirements by completing **Swegon's IT Service Provider Form** and by providing additional evidence or clarification as required.

2.1. Regulatory Compliance

The service provider shall comply with all applicable laws and regulations and shall inform Swegon of any non-EU legal obligations that may conflict with, or impact compliance with, EU laws and regulations.

In addition, where the service provider's products or services fall within the scope of specific EU regulations, the service provider shall support Swegon in fulfilling those obligations. These regulations include, but are not limited to, the General Data Protection Regulation (GDPR), the Radio Equipment Directive (RED), and the Cyber Resilience Act (CRA).

2.2. Security Framework

The service provider shall have in place a management framework for information security based on ISO 27001 or equivalent.

2.3. Roles and Responsibilities

The service provider shall have clear roles and responsibilities for information security related functions and ensure effective communication, cooperation, and coordination among those functions.

The service provider shall appoint a Single Point of Contact (SPoC) for information security who will serve as the primary liaison for all security-related communication with Swegon.

2.4. Risk Management

The service provider shall have in place procedures for identifying, classifying, and mitigating the impact of information security risks to an acceptable level.

2.5. Asset Management

The service provider shall implement processes to identify, classify, and manage all information assets, ensuring they are protected throughout their lifecycle.

2.6. Data Protection

The service provider shall handle Swegon's assets as confidential and provide an appropriate level of protection during storage and transmission.

2.7. Identity and Access Management

The service provider shall have in place an identity and access management programme that covers both logical and physical assets and that adheres to the principles of need-to-know and least privilege.

2.8. Logging and Monitoring

The service provider shall record and retain logs of activities, exceptions, faults, and other important security-related events for no less than 100 days and continuously monitor these logs for anomalies.

2.9. Security Validation

The service provider shall validate the operational security configuration and identify security gaps by performing security reviews, assessments, and testing.

2.10. Lifecycle Management

The service provider shall use technologies, protocols, and functionalities that are current and recognised as secure.

The service provider shall have implemented patch- and vulnerability management processes and apply patches in a timely manner that is aligned with the assessed level of risk.

2.11. Configuration Management

The service provider shall reduce the attack surface by implementing boundary protection, system hardening, and defence-in-depth measures.

2.12. Incident Management

The service provider shall have procedures in place to prevent, detect and respond to anomalous activity and security incidents.

The service provider shall report a security incident affecting Swegon's information, systems or services to its contact at Swegon without undue delay, and no later than 24 hours after becoming aware of it. Security weaknesses affecting Swegon shall be reported once confirmed.

2.13. Change Management

The service provider shall maintain change management processes to ensure that all changes are properly controlled.

Major changes or changes assessed to pose a high risk shall be communicated to Swegon in advance.

2.14. Continuity Management

The service provider shall maintain business continuity management procedures.

Backup copies of information shall be taken and tested according to established procedures.

Where the service provider hosts or operates a Swegon solution, they shall state the recovery time and recovery point committed to.

Restores shall be tested at least annually and the result made available to Swegon on request.

3. Exceptions

Where a requirement is not fully applicable or feasible, the service provider shall document the rationale and propose interim or compensating measures. An exception applies only once Swegon has confirmed it in writing. An agreed exception records the affected requirement, the rationale, the compensating measures and a review date.

Exceptions are time-limited where possible. An exception cannot override a legal or regulatory obligation.

4. Related Resources

The following resources are related to this document and may be consulted for further context. The Swegon guidelines and processes among them are internal documents; they are available on request.

- Swegon Information Security Policy
- Swegon Regulatory Compliance Guidelines
- Swegon Risk Assessment Guidelines
- Swegon Asset Management Guidelines
- Swegon Identity & Access Management Guidelines
- Swegon Cryptography and Key Management Guidelines
- Swegon Logging and Monitoring Guidelines
- Swegon Vulnerability Management Guidelines
- Swegon Penetration Testing Guidelines
- Swegon Secure Software Development Guidelines
- Swegon Incident Response Process
- Swegon Business Continuity Guidelines
- Swegon Security Requirements for IT Solutions
- Swegon Security Requirements for OT/ICS
- Swegon Security Requirements for Products with Digital Elements

5. References

This document is designed to support compliance with the following regulations, and is aligned with the following standards and frameworks:

Regulations

- EU General Data Protection Regulation (GDPR)
- EU Radio Equipment Directive (RED)
- EU Cyber Resilience Act (CRA)
- UK Product Security and Telecommunications Infrastructure Act (PSTI)

Standards & Frameworks

- ISO/IEC 27001, Information Security Management Systems
- NIST Cybersecurity Framework (CSF)

6. Document History

VERSION	DATE	AUTHOR	DESCRIPTION
1.8	2026-11-18	Head of Cybersecurity	References updated.
1.7	2026-11-17	Head of Cybersecurity	Scope clarified for new and existing agreements; service provider defined; deviations agreed in writing; incidents reported within 24 hours; exceptions in a section of their own.
1.6	2026-06-05	Head of Cybersecurity	Updated Scope cross-reference to include Security Requirements for Products with Digital Elements
1.5	2025-09-23	Head of Cybersecurity	Clarified scope and added proportionality and deviation process.
1.4	2025-04-17	Head of Cybersecurity	Renamed from “Third-Party Services” to “Vendors”. Removed requirement on security updates (covered by “Security Requirements for IT Solutions”). Revised Scope wording and removed redundant scope qualifiers from individual requirements.
1.3	2025-03-19	Head of Cybersecurity	Updated to align with the owner group’s cyber security baseline requirements.
1.2	2024-11-22	Head of Cybersecurity	Updated document template
1.1	2024-08-28	Head of Cybersecurity	Added Data Protection
1.0	2024-04-16	Head of Cybersecurity	First version