Swegon

Sensitivity	Public
Owner	Head of Cybersecurity
Date	2026-11-17

Swegon Security Requirements for IT Solutions

Information Security

2026-11-17 | Version 1.12



Table of Contents

1. Introduction 2
1.1. Purpose 2
1.2. Scope 2
1.3. Guidance 2
2. IT Solution Security Requirements 4
2.1. Solution Governance 4
2.2. Solution-Specific Security Requirements Engineering 4
2.3. Regulatory Compliance 4
2.4. Secure Software Development Life Cycle (SDLC) 4
2.5. Source Code Control System 5
2.6. Data Protection 5
2.7. Secrets Management 5
2.8. Transport Layer Security 5
2.9. Cryptographic Key Management 5
2.10. Authentication 5
2.11. Access Control 5
2.12. Data Validation 6
2.13. Security Libraries 6
2.14. Software Component Analysis 6
2.15. Security Logging and Monitoring 6
2.16. Secure Build & Deploy 6
2.17. Patching and Updating 6
2.18. Environment Segregation 6
2.19. Secure Configuration 6
2.20. Instructions and Documentation 6
2.21. Security Validation 6
2.22. No Known Vulnerabilities 7
2.23. Licences and Bill-of-Materials 7
2.24. Code Ownership 7
2.25. Continuity and Backup 7
3. Exceptions 8
4. Related Resources 9
5. References 10
6. Document History 11

1. Introduction

1.1. Purpose

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

This document establishes minimum technical security requirements necessary to achieve and maintain these security properties in IT solutions. The requirements are based on industry-standard frameworks such as Minimum Viable Secure Product (MVSP) and OWASP Proactive Controls.

It supplements Swegon Security Requirements for IT Service Providers and bridges the gap between high-level information security requirements and solution-specific security requirements.

1.2. Scope

The security requirements outlined in this document apply to any IT solution developed by or on behalf of Swegon, including digital services (e.g., web applications), as well as all artefacts and processes that directly or indirectly support these solutions. Products with digital elements that Swegon manufactures and places on the market are governed by Swegon Security Requirements for Products with Digital Elements.

A solution introduced before this document, or without the IT solution governance process, is brought under it through Retrospective Governance in the Swegon Asset Management Guidelines: prioritised by risk, and without waiting for that prioritisation when the solution comes forward with a request for infrastructure or access.

1.3. Guidance

Given the variability in architecture, technology stacks, and implementation details across solutions, this document does not provide specific implementation instructions or detailed technical configurations. For such guidance, developers should consult relevant platform documentation, follow industry best practices, and engage with the Head of Cybersecurity as needed to ensure compliance.

General Guidance

Developers are encouraged to reference applicable articles of the OWASP Cheat Sheet Series when implementing these requirements.

Solution-Specific Requirements

Developers are encouraged to leverage structured security requirement frameworks such as the OWASP Application Security Verification Standard (ASVS) for digital services.

Regulatory Compliance

For products with digital elements that Swegon manufactures and places on the market, refer to Swegon Security Requirements for Products with Digital Elements, which addresses applicable product regulations and the relevant harmonised standards.

Secure Software Development Life Cycle

Swegon development teams should follow the Swegon Secure Software Development Guidelines throughout the lifecycle. External suppliers are expected to maintain equivalent practices, appropriate to the scope and risk of the solution, such as those defined by NIST Secure Software Development Framework (SSDF), OWASP Software Assurance Maturity Model (SAMM) or the Microsoft Security Development Lifecycle (SDL).

2. IT Solution Security Requirements

The developer shall comply with these requirements in a manner proportionate to its organisation, the type of solution developed or maintained for Swegon, and the associated risks. These requirements shall also apply to the developer's subcontractors and third-party service providers.

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

The requirements in this document constitute a minimum; the developer shall supplement them with its own security requirements appropriate to the scope of the development and the assessed risk associated with the maintenance and use of the solution, as per section 2.2.

2.1. Solution Governance

The developer shall, upon request, demonstrate compliance with these requirements by completing **Swegon's IT Solution Requirements Form** and by providing additional evidence or clarification as required.

2.2. Solution-Specific Security Requirements Engineering

The solution shall incorporate any additional security requirements, beyond the minimum set in this document, as appropriate to the context and scope of the project.

Examples include, but are not limited to, potentially a combination of:

- **Web Applications**: HTTP security headers, e.g., Content Security Policy (CSP), Strict-Transport-Security (HSTS), secure cookie attributes, e.g., Secure, HttpOnly, and Cross-Origin Resource Sharing (CORS).
- **Cloud Solutions**: Use of cloud provider-specific security features, secure configuration of cloud services, and identity and access management (IAM) and auditing policies.

2.3. Regulatory Compliance

The applicable regulatory obligations and accountabilities are defined in the Swegon Regulatory Compliance Guidelines. For products with digital elements that Swegon places on the market, the product security requirements are defined in Swegon Security Requirements for Products with Digital Elements.

2.4. Secure Software Development Life Cycle (SDLC)

The solution shall be designed, developed, and maintained with security practices throughout its entire life cycle. This typically includes:

- **Governance:** deals with policies, risk management, and organisational aspects
- **Design:** focuses on threat modelling, security requirements and architecture reviews
- **Implementation:** addresses secure coding, reviews, and control implementation
- **Verification:** encompasses testing, validation, and security assessments
- **Operations:** covers incident management, maintenance, and improvement

Cybersecurity shall be a standing agenda item in all regular meetings between Swegon and any development teams to ensure continuous focus on secure product development.

2.5. Source Code Control System

The development team shall use a source code control system that enforces identity and access management, logs activities associated with changes to the application, and supports auditing.

2.6. Data Protection

The solution shall only store and process data that is relevant and limited to what is necessary. Where the solution processes personal data, it shall do so in accordance with the General Data Protection Regulation (GDPR) and shall support data protection by design and by default.

Sensitive data shall be separated from unprivileged storage locations.

2.7. Secrets Management

The solution shall include mechanisms to adequately protect secrets in the production environment.

2.8. Transport Layer Security

The solution shall enforce access via transport layer encryption (e.g., HTTPS/TLS) and ensure all backend communication is similarly secured.

2.9. Cryptographic Key Management

The development team shall implement cryptographic and key life cycle management practices.

2.10. Authentication

The solution shall integrate with Swegon's designated identity provider for single sign-on (SSO) and shall enforce multi-factor authentication (MFA) for all users.

The choice of identity provider is determined by the solution type and target user base:

- **Standard and commercial off-the-shelf (COTS)** solutions targeting an internal user base shall authenticate through Microsoft Entra ID.
- **Custom-built solutions** targeting an external or hybrid user base shall authenticate through Swegon Identity Server using OpenID Connect (OIDC). Where internal users require access to such solutions, Swegon Identity Server shall federate authentication to Microsoft Entra ID.

All user and system accounts, and identity provider clients, shall be separate and non-shared. Each solution shall use its own identity provider client in each environment.

2.11. Access Control

The solution shall implement a defined authorisation model (e.g., RBAC or ABAC) with documented roles and permissions.

All users, services, and application processes shall operate with the least privileges necessary, and access rights shall be reviewed periodically.

2.12. Data Validation

The solution shall validate and sanitise all input, and encode output appropriately for the target interpreter.

2.13. Security Libraries

The solution shall leverage security frameworks and libraries that embed protections against security-related design and implementation flaws.

2.14. Software Component Analysis

The development team shall perform software composition analysis (SCA) to identify potential areas of risk from the use of third-party and open-source software components.

2.15. Security Logging and Monitoring

The solution shall centrally store and monitor all relevant security-related activity.

The solution shall maintain security logs for a retention period of no less than 100 days.

2.16. Secure Build & Deploy

The development team shall utilise mechanisms for building, verifying, and deploying the software in a standardised, repeatable manner.

2.17. Patching and Updating

The development team shall ensure that all components (including third-party dependencies) are continuously kept up to date.

Security updates shall be applied (or published, where applicable) in a timely manner, consistent with the assessed level of risk and criticality of the vulnerability.

The solution shall not use any end-of-life (EOL) or unsupported components.

2.18. Environment Segregation

The development team shall provision and maintain distinct development, testing, and production environments. These environments shall be logically segregated, and physically where the risk calls for it.

2.19. Secure Configuration

The development team shall ensure that all supporting software is securely configured, hardened, and secure by default.

2.20. Instructions and Documentation

The solution shall be delivered with documentation and user instructions detailing secure configuration and usage.

2.21. Security Validation

The solution shall undergo security testing before release (verification of correctly implemented security requirements, and tool-based methods such as SAST/DAST) to discover and address security discrepancies or defects. A solution that Swegon has

classified as high criticality shall also undergo manual penetration testing by a tester independent of the development team; for other solutions it is recommended.

2.22. No Known Vulnerabilities

The solution shall be delivered without any known exploitable vulnerabilities.

Any vulnerabilities discovered after release shall be disclosed to Swegon, addressed, and remediated.

2.23. Licences and Bill-of-Materials

The development team shall comply with applicable software licences and maintain a Software Bill-of-Materials (SBOM) in a commonly used, machine-readable format.

2.24. Code Ownership

All code developed specifically for Swegon shall, unless otherwise agreed, be owned by Swegon. Code shall be considered proprietary and treated as a business secret.

2.25. Continuity and Backup

The solution shall meet defined continuity requirements based on its criticality, and backups (including source code and production data) shall be retained for a minimum of five years.

The recovery commitment of whoever provides the infrastructure shall be obtained, recorded in the solution’s disaster recovery plan, and compared with the recovery objectives of the process served. Where it falls short, the Solution Owner raises it with Swegon’s Infrastructure & Operations (I&O) team.

3. Exceptions

Where a requirement is not fully applicable or feasible, the developer 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 Identity & Access Management Guidelines
- Swegon Cryptography and Key Management Guidelines
- Swegon Logging and Monitoring Guidelines
- Swegon Vulnerability Management Guidelines
- Swegon Penetration Testing Guidelines
- Swegon Threat Modelling Guidelines
- Swegon Secure Software Development Guidelines
- Swegon Incident Response Process
- Swegon Business Continuity Guidelines
- Swegon Security Requirements for IT Service Providers
- 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 Cyber Resilience Act (CRA)

Standards & Frameworks

- NIST Secure Software Development Framework (SSDF)
- Minimum Viable Secure Product (MVSP)
- OWASP Proactive Controls
- OWASP Application Security Verification Standard (ASVS)
- OWASP Cheat Sheet Series
- OWASP Software Assurance Maturity Model (SAMM)
- Microsoft Security Development Lifecycle (SDL)

6. Document History

VERSION	DATE	AUTHOR	DESCRIPTION
1.12	2026-11-17	Head of Cybersecurity	Scope extended to existing solutions; multi-factor authentication for all users; separate identity provider clients per solution and environment; segregation of environments clarified; independent penetration testing for high-criticality solutions; exceptions in a section of their own.
1.11	2026-11-02	Head of Cybersecurity	Editorial changes.
1.10	2026-06-05	Head of Cybersecurity	Scope wording aligned.
1.9	2026-06-04	Head of Cybersecurity	Scope cross-reference to Security Requirements for Products with Digital Elements tightened.
1.8	2026-06-03	Head of Cybersecurity	Narrowed scope to IT/digital solutions; product-cybersecurity content delegated to Security Requirements for Products with Digital Elements.
1.7	2025-09-23	Head of Cybersecurity	Updated requirements for regulatory compliance and deviation process.
1.6	2025-09-10	Head of Cybersecurity	Added requirement for separate accounts and environment segregation.
1.5	2025-05-14	Head of Cybersecurity	Renamed “Custom Requirements Engineering” to “Solution-Specific Requirements Engineering”.
1.4	2025-04-23	Head of Cybersecurity	Renamed “Single Sign-On” to “Authentication”, and moved it ahead of “Access Control”.
1.3	2025-03-19	Head of Cybersecurity	Renamed from “Web Applications” to “IT Solutions” and removed web-specific requirements (should now be covered by Custom Requirements Engineering).
1.2	2025-01-22	Head of Cybersecurity	Added Requirements Engineering
1.1	2024-11-21	Head of Cybersecurity	Updated document template
1.0	2024-06-25	Head of Cybersecurity	First version