Swegon

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

Swegon Security Requirements for Products with Digital Elements

Information Security

2026-11-18 | Version 1.4



Table of Contents

1. Introduction 2
1.1. Purpose 2
1.2. Scope 2
2. Guidance 3
3. Product Security Requirements 4
3.1. Product Governance 4
3.2. Applicable Regulations and Standards 4
3.3. Product-Specific Security Requirements Engineering 5
3.4. No Default Credentials 5
3.5. Secure by Default 6
3.6. Secure Commissioning 6
3.7. Authenticated Access and Least Privilege 6
3.8. Signed and Verified Updates 6
3.9. Secure Update Delivery 6
3.10. Confidentiality of Data 6
3.11. Integrity of Data and Configuration 7
3.12. Data Minimisation 7
3.13. Attack-Surface Minimisation 7
3.14. Security Logging and Monitoring 7
3.15. Availability and Resilience 7
3.16. Secure Decommissioning 7
3.17. Software Bill of Materials 7
3.18. Coordinated Vulnerability Disclosure 8
3.19. No Known Exploitable Vulnerabilities 8
3.20. Instructions and Documentation 8
3.21. Interoperability and Integration 8
4. Exceptions 9
5. Related Resources 10
6. References 11
7. Document History 12
8. Appendix A: Product Conformity Checklist 13
8.1. Part 1: Applicability 13
8.2. Part 2: Before Placing on the Market 14
8.3. Part 3: While on the Market 15

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 security requirements for products with digital elements that Swegon manufactures, or has suppliers manufacture on its behalf, and places on the market. It supplements Swegon Security Requirements for IT Service Providers and is a sibling to Swegon Security Requirements for IT Solutions and Swegon Security Requirements for OT/ICS.

1.2. Scope

This document applies to products with digital elements that Swegon places on the market, covering the product's hardware, firmware, embedded software, and the device-side components that directly support it. Typical examples are HVAC and building-services equipment, controllers, and connected and IoT devices.

It applies in full to product types first placed on the market, or substantially modified, from the date of this version, shown on the cover. Product types already on the market, new units of them included, are brought under it retrospectively: the Product Manager, with the Head of Cybersecurity, prioritises them by risk, and a substantial modification or the next major software release brings the product under it in full. Until then, the Swegon Vulnerability Management Guidelines and the product's security support period apply, as the Swegon Regulatory Compliance Guidelines describe.

> **Note**: A product has digital elements if it incorporates software or firmware, whether or not it connects to a network.

Which document governs a given product or system depends on what Swegon does with it, not on who develops it:

- Products Swegon places on the market: this document.
- IT solutions and digital services not themselves placed on the market: Swegon Security Requirements for IT Solutions.
- Systems Swegon operates at its own production sites: Swegon Security Requirements for OT/ICS.

> **Note**: An IT solution that a product depends on for its intended functionality (a remote data processing solution under CRA Art. 3(2)) sits within the product's compliance scope and is jointly governed by this document and Swegon Security Requirements for IT Solutions.

2. Guidance

As the manufacturer, Swegon carries product lifecycle obligations that persist for the life of the product on the market. This document defines the security requirements for the product itself: it sets a minimum baseline that applies to every product with digital elements, a method for determining the additional regulations and standards that apply to a given product, and a requirement to engineer product-specific requirements on top.

> **Note**: The applicable harmonised or recognised standards are the primary source of detailed requirements; this document does not list every control a given product must meet.

The Swegon Regulatory Compliance Guidelines define the compliance governance around placing the product on the market, including conformity assessment, CE marking, mandatory reporting, the security support period, and the applicable transitional timelines such as the CRA's phased application dates.

The Swegon Secure Software Development Guidelines define how the product is securely developed.

3. Product Security Requirements

The developer shall meet the requirements in this document together with the essential requirements of the regulations and standards determined to apply under section 3.2. The legal requirements among them are mandatory for placing a product on the market. The Swegon-defined requirements are mandatory for new product types and for substantial modifications; an exception to them is handled as described in section 4. Where a regulation or standard provides its own risk-based or conditional provisions, those are applied as it specifies, not at Swegon's discretion. The requirements apply equally to the developer's subcontractors and third-party suppliers, and to internal Swegon teams where they develop a product.

Where a specific requirement is not applicable to a product, the developer shall justify and record the non-applicability in the product's cybersecurity risk assessment and technical documentation, in accordance with the Swegon Regulatory Compliance Guidelines; this forms part of the conformity process and does not waive a legal obligation.

The baseline requirements below are a minimum, supplemented by additional product-specific requirements engineered for the product.

3.1. Product Governance

Each product with digital elements shall have an assigned owner, the Product Manager, accountable for its security and regulatory compliance throughout the period it is on the market (per the Swegon Regulatory Compliance Guidelines), and a security risk classification, determined from its cybersecurity risk assessment, used to scope the product-specific requirements engineered for the product.

Security responsibility for a product stays with the Product Manager from design through end of support. Contracting the development to a supplier, buying a platform or component, or hosting a product function with a service provider does not transfer that responsibility; it is transferred only by a formal handover to another named Product Manager. The Product Manager is not expected to be a security specialist, but is expected to apply this document and to engage the Head of Cybersecurity on security decisions that exceed the product team's competence.

The developer shall, on request, demonstrate compliance with these requirements and provide additional evidence or clarification as required.

3.2. Applicable Regulations and Standards

The security and regulatory requirements that apply to a product with digital elements depend on the product's characteristics and the markets in which it is placed. Before development, the Product Manager, supported by the Head of Cybersecurity, shall determine which regulations and standards apply, in coordination with the applicability assessment defined in the Regulatory Compliance Guidelines.

The determination shall consider at least:

If the product...	**The following typically applies**	**Demonstrate conformity via**
has digital elements and is placed on the EU market	EU Cyber Resilience Act (CRA) essential requirements	Harmonised standards once published; until then ETSI EN 303 645 and IEC/EN 62443-4-2

If the product...	The following typically applies	Demonstrate conformity via
incorporates a radio interface (Wi-Fi, Bluetooth, cellular, etc.)	EU Radio Equipment Directive (RED) Art. 3(3)(d)(e)(f)	EN 18031-1/-2/-3 as applicable (network protection, personal data, fraud)
is machinery or a safety component	EU Machinery Regulation cyber-safety requirements	Harmonised standards; a cybersecurity certificate under the Cybersecurity Act gives presumption of conformity
generates data accessible to users	EU Data Act data-access-by-design obligations	Documented data-access design (no harmonised standard; see Regulatory Compliance Guidelines)
includes AI-enabled features	EU AI Act risk classification and, where high-risk, the high-risk requirements	Harmonised standards / EU AI Act conformity route
is sold to UK consumers	UK PSTI security requirements	ETSI EN 303 645 provisions per the PSTI Regulations
is intended for consumers or likely to be used by them	EU General Product Safety Regulation (GPSR) safety requirements, including cybersecurity that protects safety	Safety assessment and technical documentation under the GPSR; the Machinery rules take precedence where they apply
is placed on the EU market (any product, from 9 December 2026)	EU Product Liability Directive (PLD): a cybersecurity defect or a missing update is a product defect	No conformity route; technical documentation and the update record are the defence

3.3. Product-Specific Security Requirements Engineering

The minimum product security baseline set out below is a floor and is not sufficient on its own to demonstrate conformity. Each product shall incorporate additional security requirements appropriate to its context, derived from the applicable standards identified in section 3.2 and from threat modelling and risk assessment of the product, and engineered using structured catalogues such as the OWASP ISVS and ASVS, proportionate to the product's risk classification.

Threat modelling shall follow the Swegon Threat Modelling Guidelines, and the product shall be designed, developed, and maintained in accordance with the Swegon Secure Software Development Guidelines throughout its lifecycle.

External suppliers are expected to maintain equivalent secure-development practices, such as those defined by the NIST Secure Software Development Framework (SSDF), OWASP Software Assurance Maturity Model (SAMM), or the Microsoft Security Development Lifecycle (SDL).

The following baseline requirements apply to every product with digital elements, regardless of which additional regulations or standards apply.

3.4. No Default Credentials

The product shall not use universal default credentials. Passwords shall be unique to each unit (device) or set by the user on first use, and shall not be derivable from public information

or product identifiers. Where credentials are set on first use, the initial setup process shall be protected so that the product is not left exposed during the period before it is configured.

3.5. Secure by Default

The product shall be shipped in a hardened, secure-by-default configuration, with unused functionality disabled, and shall allow the user to reset it to its original (factory-default) secure state.

3.6. Secure Commissioning

Where the product is brought into operation by an installer or service technician, the commissioning process shall be authenticated and shall leave the product in a secure operational state, including replacing any provisioning or temporary credentials (which are subject to No Default Credentials) and confirming secure configuration, before handover to the customer.

3.7. Authenticated Access and Least Privilege

The product shall protect against unauthorised access through appropriate authentication and access-control mechanisms, and shall enforce least privilege across its interfaces, services, and processes. Authentication mechanisms shall be protected against automated and brute-force attempts, for example through rate-limiting or progressively increasing authentication delays. The product shall support multi-factor authentication on its administrative and high-privilege interfaces (including remote, cloud-based, and local service or commissioning interfaces) where technically feasible. Hard-coded credentials, backdoor codes, and undocumented access paths are prohibited.

3.8. Signed and Verified Updates

Software and firmware updates shall be cryptographically signed and verified before installation, in accordance with the Swegon Cryptography and Key Management Guidelines. Where the hardware platform supports it, the product shall verify firmware authenticity before execution (secure boot), and shall revert to a known-good state on update failure. The update mechanism shall prevent rollback to known-vulnerable earlier versions. The product shall be designed for cryptographic agility so that the cryptographic algorithms and keys it uses (for update signing, secure communication, and data storage) can be updated in the field over its supported lifetime.

3.9. Secure Update Delivery

The product shall provide a mechanism to distribute security updates to the product in a secure and timely manner, automatically where appropriate to the product type. Where automatic updates are provided, they shall be enabled by default, with a clear and easy-to-use opt-out, notification of available updates to the user, and the option to postpone them temporarily. Security updates shall be provided free of charge and, where technically feasible, separately from functionality updates, accompanied by information on the issue addressed and any recommended action.

3.10. Confidentiality of Data

The product shall protect the confidentiality of sensitive data it stores, processes, or transmits, including encryption in transit and at rest using current algorithms in accordance with the Swegon Cryptography and Key Management Guidelines.

3.11. Integrity of Data and Configuration

The product shall protect the integrity of stored and transmitted data, commands, and configuration against unauthorised manipulation, and shall be able to report detected corruption. The product shall maintain a trustworthy time source, for example through secure time synchronisation, where accurate time is needed for certificate validation, log timestamping, or update verification.

3.12. Data Minimisation

The product shall process only data that is adequate, relevant, and limited to what is necessary for its intended purpose. Where the product processes personal data, it shall support data protection by design and by default in accordance with the Swegon Group General Personal Data Policy.

3.13. Attack-Surface Minimisation

The product shall limit its attack surface by disabling unused interfaces, services, and ports. Physical debug and test interfaces (for example JTAG, UART, or SWD) shall be disabled or access-protected on production units. Products shall be released with release-build firmware and configuration, with no debug code or privileged diagnostic functionality enabled.

3.14. Security Logging and Monitoring

The product shall record security-relevant events (such as access to and modification of data, services, or functions, changes to installed software or configuration, and indicators of possible unauthorised access) in accordance with the Swegon Logging and Monitoring Guidelines, where the product technically supports it. Such events shall be retained on the product at least long enough to be reliably exported to a configured collector, with longer-term retention and analysis provided via that export path (see Interoperability and Integration), and shall be capable of being examined to detect and report security-relevant conditions.

3.15. Availability and Resilience

The product shall protect the availability of its essential functions, including resilience against and mitigation of denial-of-service conditions, and shall minimise any negative impact it may have on the services of other devices or networks. The product shall remain functional for its essential local functions during loss of network connectivity and recover cleanly to a secure operational state after power or connectivity is restored.

3.16. Secure Decommissioning

The product shall allow the user to securely and permanently remove all data and settings, and to securely transfer such data where transfer is supported, when the product is decommissioned or changes ownership.

3.17. Software Bill of Materials

The developer shall identify the components contained in the product and maintain a Software Bill of Materials (SBOM) in a commonly used, machine-readable format covering at least the top-level dependencies, and transitive dependencies where tooling allows.

3.18. Coordinated Vulnerability Disclosure

The product shall be covered by a coordinated vulnerability disclosure capability, including a published contact point for reporting vulnerabilities and a process for handling reports, in accordance with the Swegon Vulnerability Disclosure Policy. Affected users shall be informed of a resolved vulnerability and of the measures they can take. Security advisories are published as the Swegon Vulnerability Management Guidelines describe, where appropriate in a machine-readable format (for example CSAF/VEX).

3.19. No Known Exploitable Vulnerabilities

The product shall be placed on the market without known exploitable vulnerabilities. The developer shall apply effective and regular security testing appropriate to the product type, including penetration testing where appropriate in accordance with the Swegon Penetration Testing Guidelines. The product's components shall be continuously monitored for newly disclosed vulnerabilities (for example, against the SBOM) throughout the support period. Vulnerabilities discovered after release shall be disclosed to Swegon, addressed, and remediated within the support period in accordance with the Swegon Vulnerability Management Guidelines.

3.20. Instructions and Documentation

The product shall come with clear instructions for installing, operating, updating and decommissioning it securely, in a format Swegon can retain and provide for the required period.

3.21. Interoperability and Integration

Where appropriate to the product type, the product should be designed to integrate securely into the customer's operational and security environment, not only Swegon's. It should:

- Support exporting its security-relevant logs and events to a customer-designated collector using open, standard protocols (for example syslog, MQTT, or webhook/OpenTelemetry), so that customers can ingest them into their own monitoring or SIEM platform.
- Support standards-based identity federation for management interfaces (for example OIDC or SAML) so that the product can be integrated into the customer's identity provider rather than relying solely on local accounts.
- Support standards-based network admission (for example 802.1X) so that the product can authenticate to the customer's network access control.
- Expose any management or integration APIs securely (authenticated, authorised, and rate-limited) and document them.

Where the product connects to Swegon's Digital Service Platform, it shall authenticate using its unique device certificate over mutual TLS, as defined in the Swegon Digital Certificate Issuing Guidelines and the Swegon Cryptography and Key Management Guidelines.

4. Exceptions

Where the developer cannot meet a Swegon-defined requirement that goes beyond the applicable legal requirements (for example the Digital Service Platform integration requirement) for a specific product, the developer shall document the rationale and propose compensating measures. An exception applies only once Swegon has confirmed it in writing and accepted the remaining risk. An agreed exception records the affected requirement, the rationale, the compensating measures and a review date.

Exceptions are time-limited where possible. A legal requirement cannot be waived in this way.

5. 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 Group General Personal Data Policy
- Swegon Regulatory Compliance Guidelines
- Swegon Risk Assessment Guidelines
- Swegon Threat Modelling Guidelines
- Swegon Secure Software Development Guidelines
- Swegon Cryptography and Key Management Guidelines
- Swegon Digital Certificate Issuing Guidelines
- Swegon Logging and Monitoring Guidelines
- Swegon Vulnerability Management Guidelines
- Swegon Vulnerability Disclosure Policy
- Swegon Penetration Testing Guidelines
- Swegon Incident Response Process
- Swegon Business Continuity Guidelines
- Swegon Security Requirements for IT Solutions
- Swegon Security Requirements for IT Service Providers
- Swegon Security Requirements for OT/ICS

6. 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)
- EU Radio Equipment Directive (RED)
- EU Machinery Regulation
- EU Data Act
- EU AI Act
- UK Product Security and Telecommunications Infrastructure Act (PSTI)
- EU General Product Safety Regulation (GPSR)
- EU Product Liability Directive (PLD)

Standards & Frameworks

- OWASP IoT Security Verification Standard (ISVS)
- OWASP Application Security Verification Standard (ASVS)
- NIST Secure Software Development Framework (SSDF)
- OWASP Software Assurance Maturity Model (SAMM)
- Microsoft Security Development Lifecycle (SDL)
- EN 18031-1:2024, Common security requirements for internet-connected radio equipment
- EN 18031-2:2024, Common security requirements for radio equipment processing personal, traffic, or location data
- EN 18031-3:2024, Common security requirements for radio equipment processing virtual money or monetary value
- ETSI EN 303 645, Cyber Security for Consumer Internet of Things
- IEC/EN 62443-4-2, Technical security requirements for IACS components

7. Document History

VERSION	DATE	AUTHOR	DESCRIPTION
1.4	2026-11-18	Head of Cybersecurity	Editorial changes; no change to the requirements.
1.3	2026-11-17	Head of Cybersecurity	Scope clarified for products already on the market and by product type; support period of at least five years; users informed of resolved vulnerabilities; passwords unique to each unit; conformity route and automatic updates as the Cyber Resilience Act states them; exceptions in a section of their own.
1.2	2026-10-28	Head of Cybersecurity	GPSR and PLD rows added to Applicable Regulations and Standards; product ownership principle added to Product Governance; Appendix A, Product Conformity Checklist, added
1.1	2026-06-05	Head of Cybersecurity	Interoperability and Integration section moved after the baseline requirements.
1.0	2026-06-03	Head of Cybersecurity	Initial version

8. Appendix A: Product Conformity Checklist

The Product Manager shall complete this checklist with the Security Champion (a role defined in the Swegon Secure Software Development Guidelines) at three points: when the product is defined or materially changed (Part 1), before it is placed on the market or substantially modified (Part 2), and on a recurring basis while it is on the market (Part 3). The completed checklist and the evidence it points to shall be retained with the product's technical documentation and made available on request; it is how the developer demonstrates compliance under Product Governance.

The checklist does not decide whether a regulation applies. Where applicability turns on a legal interpretation rather than a security judgement, the Product Manager escalates it as the Regulatory Compliance Guidelines describe. For an item, or the part of it, that goes beyond what a regulation requires, an exception may be agreed as described under Exceptions. For a legal requirement it may not.

8.1. Part 1: Applicability

Record the product's answers to the table in section 3.2, Applicable Regulations and Standards (placed on the EU market; radio interface; machinery or safety component; data accessible to users; AI-enabled features; sold to UK consumers; intended for or likely to be used by consumers), and to the questions below, and keep them with this checklist. Together they determine which rows of Parts 2 and 3 apply to the product and which conformity route it takes. Revisit them at every material change.

Does the product...	**If yes**	**Record**
have a network interface, so that it can communicate over a network and, directly or through other equipment, over the internet?	Treat it as exposed, whatever the intended installation: RED Art. 3(3)(d) and EN 18031-1 where it has a radio interface; CRA Annex I attack-surface requirements; High criticality (Secure Software Development Guidelines); penetration test (Part 2)	The intended operational environment (isolated, behind a gateway, internet-facing), stated in the deployment guidance; the exposure assumed in the risk assessment
process personal, traffic or location data?	RED Art. 3(3)(e) and EN 18031-2 where it has a radio interface; GDPR data protection by design and the Swegon Group General Personal Data Policy	The data categories; the DPO consulted
process virtual money or monetary value?	RED Art. 3(3)(f) and EN 18031-3 where it has a radio interface	The payment function
depend on a remote data processing solution for its intended functionality?	That solution is within the product's CRA scope (CRA Art. 3(2)) and is assessed jointly with Swegon Security Requirements for IT Solutions, as the Scope section describes	The solution and its Solution Owner

Does the product...	If yes	Record
fall within a CRA Annex III or Annex IV product class?	The conformity assessment route CRA Art. 32 sets for the class: for class I, self-assessment only where harmonised standards, common specifications or a certification scheme are applied in full; otherwise, and for class II and Annex IV, third-party assessment or certification	The class and the route chosen
carry Swegon's name or trademark as an imported product, or has it been substantially modified by Swegon after being placed on the market?	Swegon carries the manufacturer obligations for the product (Regulatory Compliance Guidelines), on the same route as a product Swegon manufactures	The original manufacturer; the modification

8.2. Part 2: Before Placing on the Market

Complete before the product is first placed on the market, and again after any substantial modification.

Item	Completion criteria	Applies when
Owner and classification	Product Manager named; security risk classification set from the cybersecurity risk assessment	Always (Swegon)
Conformity route	Self-assessment or notified body decided and justified; notified body report on file where used	Radio interface (RED); CRA Annex III or IV class
Cybersecurity risk assessment	Documented, covers design through maintenance, kept updated; every requirement judged not applicable is justified in it	Always (CRA Art. 13(2))
Threat model	Current; high-priority mitigations implemented	Always (Secure Software Development Guidelines)
Product-specific requirements	Engineered from the applicable standards and the threat model; traced to implementation	Always (this document)
Baseline requirements	Each baseline section of this document confirmed met; exceptions agreed as described under Exceptions	Always (this document)
Standard conformity evidence	EN 18031 decision trees and justifications per mechanism; CRA mapping to the harmonised standard, or to ETSI EN 303 645 or IEC 62443-4-2 until one is published	Radio interface (RED); always (CRA)
Release checklist	Secure Software Development Guidelines Appendix A completed for the release build	Always (Secure Software Development Guidelines)

Item	Completion criteria	Applies when
Penetration test	Completed on the release candidate; critical and high findings fixed; attestation on file	Connectable product (High criticality under the Secure Software Development Guidelines); recommended otherwise
Known vulnerabilities and SBOM	No publicly known exploitable vulnerability at release; SBOM current and machine-readable	Always (CRA Annex I)
Secure update path	Updates signed and verified, rollback prevented, delivery channel tested end to end	Always (CRA; RED SUM where radio)
Credentials	No universal default credentials; commissioning replaces provisioning credentials	Always (CRA; RED AUM and CCK where radio; PSTI)
Support period	Defined, documented and published: at least five years, set with regard to the time the product is expected to be in use	Always (CRA Art. 13(8); PSTI; Regulatory Compliance Guidelines)
User documentation	Instructions to install, operate, update and decommission securely; retained for the required period	Always (CRA Annex II)
Vulnerability disclosure	Product within the scope of the Vulnerability Disclosure Policy; advisory channel chosen	Always (CRA; PSTI)
Reporting readiness	Product Manager knows the Single Reporting Platform route and the Incident Response Process; submitter named	Always (CRA Art. 14, applicable since 11 September 2026)
Technical documentation	Per CRA Annex VII and, where radio, RED Annex V; retained ten years after placing on the market or for the support period, whichever is longer	Always (CRA Art. 13; RED)
Other acts	PSTI statement of compliance; GPSR safety assessment; Data Act access design and sharing records; AI Act classification and, where high-risk, conformity documentation; Machinery cyber-safety evidence	As the Part 1 answers indicate
Declaration and marking	EU declaration of conformity issued, listing each applicable act; CE marking applied	Always (RED now; CRA from 11 December 2027)
Sign-off	Product Manager signs; Business Owner informed; Head of Cybersecurity informed, and consulted where the design was high-risk	Always (Swegon)

8.3. Part 3: While on the Market

Recurring items for the support period. A substantial modification triggers Part 2 again.

Item	Completion criteria	When
Vulnerability monitoring	SBOM components monitored; findings remediated within the Vulnerability Management Guidelines timelines; affected users informed	Continuous

Item	Completion criteria	When
Security updates	Available and delivered for the whole support period, free of charge	Continuous
Reporting	Actively exploited vulnerabilities and severe incidents reported within the CRA Art. 14 timelines; affected users informed	On occurrence
Risk assessment and threat model	Reviewed on material change and at least yearly; technical documentation updated	Yearly, or on change
Data access requests	Users' requests for the data the product generates handled as the Data Act requires; sharing arrangements recorded	On request (Data Act), where the product generates user-accessible data
AI post-market monitoring	For a high-risk AI feature: the post-market monitoring plan operated; serious incidents reported to the market surveillance authority	Continuous (AI Act), where high-risk
Substantial modification	Assessed against the CRA definition; Part 2 repeated where it applies; declaration reissued	On change
End of support	Users informed in advance; final security communication issued; technical documentation updated	At end of support