Swegon

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

Swegon Security & Trust Overview

Information Security

2026-11-18 | Version 1.0



Table of Contents

1. Introduction 2
2. Security Governance 2
3. Our Approach to Security 3
4. People & Security Culture 3
5. Risk & Asset Management 4
6. Secure Development 4
7. Vulnerability Management & Coordinated Disclosure 4
8. Incident Response & Resilience 5
9. Supply Chain & Third-Party Security 5
10. Data Protection & Privacy 5
11. Standards, Certifications & Regulatory Alignment 5
12. Security Inquiries 6
13. Cybersecurity Disclaimer 8

1. Introduction

Swegon is dedicated to ensuring that our solutions, operations and practices are effective, sustainable and secure, with a commitment to safeguarding data and supporting trust in everything we do. As our products and services become more connected, cybersecurity is integral to that commitment.

This overview describes how Swegon approaches security as an organisation: our governance, the way security is built into our products and services, and the programmes through which we manage risk, vulnerabilities and incidents. It is intended to support customers, procurement teams and partners in evaluating Swegon as a trustworthy supplier.

It is the top of three layers of the security documentation Swegon provides to customers:

- **Swegon Security & Trust Overview (this document)**: how Swegon approaches security as an organisation.
- **Connected Products Security & Secure Deployment Guide**: how to deploy and operate connected Swegon products securely, across the portfolio.
- **Each product's own documentation**, including a dedicated Security & Trust Overview where published: the product specifics (security architecture, interfaces, defaults and version-specific behaviour) and assessment or certification evidence.

> **Scope and limitations:** This is a general description of Swegon's security programme, not a warranty and not a substitute for contractual terms, product documentation, security advisories or a customer's own risk assessment. Product capabilities vary and evolve; the authoritative detail for any product or service is its own product documentation, a dedicated Security & Trust Overview where published, or otherwise Swegon, contacted as described in section 12.

2. Security Governance

Security is governed through a formal Information Security Management System (ISMS) that establishes the framework for managing risk, protecting assets and meeting regulatory and contractual obligations. The ISMS applies across all Swegon entities, including subsidiaries, and extends to employees, consultants, partners and third parties who manage or access Swegon's assets; implementation reflects local operations, risk and regulatory context. It is supported by topic-specific policies, guidelines, requirements and processes, and is subject to continual improvement driven by risk assessments, incident reviews, internal audits, management reviews and regulatory developments.

Accountability. Information security has executive-level accountability at Group level, with a dedicated Head of Cybersecurity owning cybersecurity governance, policy and risk management and maintaining the ISMS. Consistent with Swegon's governance model, defined responsibilities are distributed across business owners, solution owners and product managers, operations and local IT roles, development teams, and every employee, so that security is owned where decisions are made, throughout each solution's or product's lifecycle.

Objectives. The ISMS pursues clear objectives: systematic, standards-aligned risk management; accountability for everyone who handles information; and a strong security culture from leadership to every employee, supported by measurable indicators such as awareness-training completion, incident detection and response times, and timely

remediation of critical and high vulnerabilities. Objectives and policies are reviewed at least annually and when significant change occurs.

Assurance and maturity. The ISMS is established, with a defined internal audit programme and management review. Swegon has carried out structured gap assessments against ISO/IEC 27001 and the NIS2 Directive and maintains a prioritised remediation roadmap that drives continual improvement.

3. Our Approach to Security

Effective security must be embedded from the start, woven into every stage of development and operation. Our approach rests on four principles:

- **Security by design**. Security is considered from the first architecture decision, to keep the attack surface small: threat modelling before development, and independent penetration testing, particularly for customer-facing and sensitive systems.
- **Security by default**. Swegon's products ship with secure defaults wherever interoperability with existing building systems allows, and newer software is replacing shared factory passwords with unique or user-set credentials; connections from Swegon's products to its cloud services are encrypted and mutually authenticated. Building-automation protocols without authentication of their own remain enabled for interoperability. Each product's documentation states what applies to it, and what the network must provide.
- **Defence in depth**. Multiple independent layers protect systems and products, so that no single failure exposes the whole: authentication and role separation, logging, and the segmented network the installation provides.
- **Continuous improvement**. Security measures are reviewed and updated as threats and best practice evolve: vulnerability sources are monitored, the vulnerabilities Swegon finds or is told about are handled, and reports are invited through the Vulnerability Disclosure Policy.

> **Note**: Security in a connected building is a shared effort. Swegon secures the products and services it provides and gives guidance for the environment they run in; the customer secures that environment. The Connected Products Security & Secure Deployment Guide sets out who does what.

4. People & Security Culture

Security depends on people as much as technology. All personnel with access to Swegon's information systems, including permanent employees, temporary staff and contractors, are required to complete security awareness training and to acknowledge Swegon's security policy as part of onboarding.

Awareness is maintained through a continuous programme of micro-training and simulated phishing. Acceptable-use rules, information-handling expectations and clear channels for reporting risks and incidents apply across the organisation.

5. Risk & Asset Management

Swegon follows a structured process to identify, analyse, evaluate and treat risks to information assets. Risks requiring active management are recorded with an owner and a treatment plan, and residual risk is accepted at an authority level matching its severity.

IT solutions are required to pass a defined governance process, which evaluates security and compliance, before they are introduced. The process covers assets throughout their lifecycle, from onboarding through decommissioning. Information is classified by sensitivity, with handling rules applied from the point of creation.

6. Secure Development

Security is integrated across the development lifecycle. Minimum technical security requirements apply to the IT solutions Swegon develops and to the products Swegon manufactures and places on the market; for a product, they are determined by the standards and regulations that apply to it, listed under Standards, Certifications & Regulatory Alignment. Secure development practices define the required security activities at each phase, from planning and design through release, operations and decommissioning, covering secure coding, secrets management, pipeline security and testing.

Cryptography follows defined minimum standards for algorithms, key management and PKI, with connected-product certificates issued from a dedicated private certificate authority on a managed PKI platform.

7. Vulnerability Management & Coordinated Disclosure

Swegon manages vulnerabilities across infrastructure, digital services, OT/ICS systems, third-party services and the products it manufactures. The process covers discovery, severity classification, prioritised remediation within defined target timelines, and coordinated vulnerability disclosure.

Swegon’s security advisories identify the affected products and versions, the severity and potential impact, and mitigation or remediation steps, and may reference a CVE so customers can track the issue. Advisories are published on the Swegon security pages (swegon.com/security) and through the channels in which the product’s software updates and documentation are published. For manufactured products, vulnerability handling and disclosure form part of Swegon’s manufacturer obligations under applicable regulations. Where Swegon has defined a minimum security update support period for a connected product, security updates and vulnerability fixes are provided during it; the period is stated in the product’s Security & Trust Overview or other product documentation.

External security researchers are encouraged to report vulnerabilities through Swegon’s Vulnerability Disclosure Policy; Swegon also operates scoped, invitation-based security testing for selected systems.

8. Incident Response & Resilience

Swegon operates a documented incident response process aligned with recognised standards, spanning preparation, detection, triage, containment, remediation, recovery and lessons learned. Security events across Swegon's managed environment are monitored on a 24/7 basis by a dedicated security-operations partner, which also performs active threat hunting and provides rapid-response and forensic capability. Incidents are classified by severity with defined escalation paths.

Where an incident or an actively exploited vulnerability could affect customers, Swegon promptly informs the affected users it can identify directly, and all users through the channels in which its security advisories are published, tells them what measures they can take, and makes any required notifications to the relevant authorities, consistent with applicable regulations such as GDPR, NIS2 and the EU Cyber Resilience Act. Customers who suspect a security incident involving a Swegon product or service can contact Swegon at security@swegon.com. Business continuity plans are required for business-critical processes and the solutions that support them.

9. Supply Chain & Third-Party Security

Swegon sets security requirements for its suppliers and service providers, addressing security frameworks, risk management, data protection, access controls, incident reporting and business continuity, and requires them to be passed on to subcontractors. The requirements are carried into supplier agreements as these are entered into or renewed, and provide for a security evaluation of the provider when an IT solution or service is introduced.

10. Data Protection & Privacy

Swegon protects the confidentiality, integrity and availability of the data it holds, and processes personal data in line with the EU General Data Protection Regulation (GDPR); see Swegon's privacy policy for how personal data is collected and used. Swegon's corporate and cloud-hosted connected-product services are primarily operated within the EU. Where a specific service, subprocessor, backup, logging or support component is arranged differently, this is confirmed through product documentation, contractual terms or on request.

Data-protection obligations are assessed for the products and services Swegon provides. Product- and service-specific data handling is described in the relevant product documentation or available on request, as described in section 12.

11. Standards, Certifications & Regulatory Alignment

Swegon identifies and tracks the standards and regulations relevant to our security work. The main ones are listed below, grouped according to how they apply.

References to ISO/IEC 27001 in this document describe alignment, not certification, unless certification is explicitly stated in product-, service- or entity-specific documentation.

Frameworks we align our ISMS and engineering with:

- **ISO/IEC 27001**: information security management
- **NIST Cybersecurity Framework**: risk management and security controls
- **OWASP ASVS and ISVS, the OWASP Proactive Controls and Minimum Viable Secure Product**: the technical baseline of Swegon's security requirements for IT solutions and products

Standards our connected products are assessed or designed against:

- **EN 18031 series**: for the cybersecurity requirements of the EU Radio Equipment Directive, where applicable
- **IEC 62443**: designed with reference to the IACS component requirements of IEC 62443-4-2
- **ETSI EN 303 645**: reference for consumer IoT security, and for the Cyber Resilience Act until harmonised standards are published

Product regulation, as each applies to a product:

- **EU Radio Equipment Directive (2014/53/EU)**: manufacturer obligations for radio equipment
- **EU Cyber Resilience Act (CRA)**: manufacturer obligations for products with digital elements
- Further product regulation tracked and addressed as applicable (e.g. PSTI, AI Act, Data Act)

Regulation that applies to Swegon as an organisation:

- **EU NIS2 Directive**: security and incident-reporting obligations; NIS2 applies to organisations rather than to products
- **EU GDPR**: personal-data protection

Product-specific assessment or certification evidence, where it exists, is described in the product's documentation or its Security & Trust Overview where published, which says what is available on request and what only under NDA.

12. Security Inquiries

Swegon's security documentation is available from the Swegon security pages (swegon.com/security): this overview, the Connected Products Security & Secure Deployment Guide, and the published product Security & Trust Overviews and security requirements.

Where to find what:

Need	Where
General security posture	This Security & Trust Overview
Deploying and operating connected products	Connected Products Security & Secure Deployment Guide
A specific product's security detail	That product's Security & Trust Overview, where published
Known vulnerabilities and fixes	Security advisories, linked from swegon.com/security

Need	Where
Reporting a vulnerability	Vulnerability Disclosure Policy (swegon.com/security/vulnerability-disclosure-policy)
Suspected security incident involving a Swegon product or service	security@swegon.com

For detailed security inquiries or requests for additional documentation, please contact your Swegon sales representative, or Swegon at swegon.com/contact; the request is passed to Swegon's cybersecurity function and the product team as appropriate.

A more detailed Security Assurance Summary is available to customers under NDA on request. It is aligned with ISO/IEC 27001 and includes a control-by-control mapping to Annex A controls to support security questionnaires.

13. Cybersecurity Disclaimer

Swegon provides products, solutions and services that include security functions supporting the secure operation of building systems. Protecting systems against cyber threats requires implementing and continuously maintaining a holistic security concept, of which Swegon's portfolio forms one element. You are responsible for preventing unauthorised access to your systems, which should only be connected to networks or the internet when necessary and with appropriate security measures in place. Swegon strongly recommends applying software updates as soon as they are available and using the latest product versions; use of unsupported versions or failure to apply updates may increase exposure to cyber threats.