External Product Security Policy

Product Security Function

Version 2.0

Date: 2023-11-20

aaesproduct.security@assaabloy.com

Purpose

The External Product Security Policy aims to define a framework for protecting the security properties of our assets and to assure our customers and other interested parties that we adequately manage information security risks.

Scope

This policy applies to customers, suppliers, regulators, and other interested third parties.

Policy Requirements

People

- **Screening**: We perform background verification checks on all new employees and consultants.
- **Employment Contract**: Our employment contract defines each party's obligations regarding information security.
- **Training and Awareness**: All employees and consultants participate in our information security and awareness program.
- **Disciplinary Process**: Any employee or consultant who violates the Product Security Policy may be subject to disciplinary action and up to and including termination of employment.

Secure Framework

Our security framework covers:

- **Secure Development Process:** Risk-based security by design approach for classifying information and related assets to determine criticality and ownership, assess threat and manage risk, ensure secure coding, and define protection requirements.
- **Vulnerability Management:** Through our vulnerability disclosure policy and vulnerability handling process, we improve overall security and build customer trust in our products by proactively identifying and mitigating potential vulnerabilities.
- **Incident Management:** We detect, assess, classify, remediate, respond, and learn from security events and incidents via our incident handling process.
- **Readiness and Continuity:** We follow the Plan, Do, Check, and Act framework that ensures that our products are resilient and recoverable within agreed pre-determined levels and timelines.
- **Compliance:** We identify, maintain, and comply with relevant laws, regulations, and standards, including:
- GDPR
- European standard (EN 303 645) on Cyber; Cyber Security for Consumer Internet of Things: Baseline Requirements
- ISO/IEC 27001:2022 and ISO/IEC 27002:2022
- NIST Special Publication
- OWASP ASVS Standard
- CIS AWS Foundations Benchmark
- AWS Foundational Security Best Practices

Physical Facility

We define and implement physical controls to protect our site, equipment, personnel, and systems from potential danger or damage.

Supplier Relationship

We evaluate supplier relationships to mitigate information security risks.

Authentication and Authorization

Our systems securely authenticate and authorize users, devices, services, and programs before granting access.

Cryptography

We deploy consensus and secure cryptographic algorithms to protect the security properties of our assets.

Technology Controls

We assess and implement necessary security controls to preserve the confidentiality, integrity, and availability of information and related assets.

Performance Evaluation

We define and evaluate the key performance indicators tied to our security objectives to ensure the realization of the intended information security management system outcomes.

Continual Improvement

We continually review and improve our information security management system.