SUPPLIER SHIELD

Vulnerability Management Policy

Rue de la gare 39 | 1110 Morges | Switzerland | T +41 21 802 35 54 | request@suppliershield.com
https://www.suppliershield.com/

Table of Contents

1. Purpose

This policy outlines Supplier Shield™ objectives and methodology to manage vulnerabilities within the organization's AWS-hosted environment. It is intended for external audiences requiring visibility in our framework for identifying, assessing, and remediating vulnerabilities across applications, systems, and networks. While the governance responsibilities, tools, and response timelines required to protect the confidentiality, integrity, and availability of our assets are presented, Supplier Shield™ reserves the right to omit confidential information that may compromise the employees, stakeholders or company's security and privacy.

Supplier Shield™ has developed a vulnerability management process with a risk-based approach to managing information security and privacy across the organization and protect its information, resources, and systems.

This policy promotes alignment with industry best practices and ISO/IEC 27001:2022 through the integration of principles such as zero-trust architecture, privacy by design, privacy by default, and the CIS Security Benchmarks. The policy guarantees uniform implementation of security controls across all business functions.

2. Scope

This policy applies to all Supplier Shield™ personnel, processes, and systems operating within the AWS-managed infrastructure.

The policy encompasses:

- Supporting systems, including applications, databases, and cloud environments.
- Personnel, including employees, contractors, and key third-party partners.
- Processes, procedures, and other relevant documented information that contribute to the protection of information assets.

More specifically, it includes:

- All internet-facing and internal applications.
- The underlying infrastructure components supporting these applications and services.
- Personnel responsible for vulnerability management, including those tasked with identifying, responding to, and remediating vulnerabilities.
- Third-party services and tools integrated into the environment.

3. Definitions

Term / Abbreviation	Definition
AWS Security Hub	A security service that provides a comprehensive view of security alerts and compliance status within AWS.
Availability	Characteristic of the information by which authorized persons can access when it is needed.
CIS Benchmarks	Security configuration best practices published by the Centre for Internet Security (CIS).
Confidentiality	Characteristic of the information by which it is available only to authorized persons or systems.
Information Security Management System (ISMS)	System to manage risks related to the security of information an organization own or handle.
Integrity	Characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.
Penetration Test (Pentest)	A simulated cyberattack used to identify and assess exploitable vulnerabilities.
SNS (Simple Notification Service)	An AWS web service that manages and sends alerts related to vulnerability findings.
Steering Committee (SteerCo)	Information Security Steering Committee responsible for overseeing the effective implementation of the Information Security Program (ISP), and ensuring that the confidentiality, integrity, and availability of Supplier Shield™ systems and data are maintained.
Threat	Potential cause of an unwanted incident, which can result in harm to a system or organization.
Vulnerability	Weaknesses of an asset or control that can be exploited so that an event with a negative consequence occurs.

4. Roles & Responsibilities

Chief Executive Officer (CEO)

- Ensures executive oversight of the vulnerability management program.
- Reviews and approves remediation priorities for critical vulnerabilities.
- Allocates appropriate resources and support to enable timely remediation and risk mitigation.

Product Development Director

- Coordinates periodic vulnerability and penetration testing activities.
- Ensures that identified vulnerabilities in products and environments are remediated within approved timelines.
- Reviews product initiatives to assess and mitigate security risks.
- Reports on maturity control and recommends secure technology improvements.

Quality Assurance (QA)

- Provides confidence that development characteristics and deliverable fulfills requirements.

Information Security Officer (ISO):

- Disseminates relevant threat intelligence and performs ongoing threat and vulnerability monitoring.
- Coordinates with system owners and product teams for vulnerability patching and change management.
- Monitors and escalates unresolved critical issues to executive management.

ISMS Manager:

- Ensures that information security best practices are defined, implemented, and maintained across the organization.
- Maintains policies, procedures, and records related to risk treatment and vulnerability management.
- Ensures results feed into risk assessments, management reviews, and continuous improvement initiatives.

5. Vulnerability Management Controls

Supplier Shield™ adopts a proactive and structured approach to vulnerability management by leveraging automated tools, external threat intelligence, and regular penetration testing to identify, assess, and remediate security weaknesses.

The Supplier Shield™ platform is hosted and managed within the AWS environment. Vulnerability monitoring is performed through AWS Security Hub, which is configured in accordance with the CIS AWS Foundations Benchmarks and AWS Foundational Security Best Practices to ensure continuous compliance and effective security posture management.

a. Threat Intelligence

The Information Security Officer (ISO) is responsible for continuously monitoring external sources to identify new vulnerabilities and emerging cybersecurity threats.

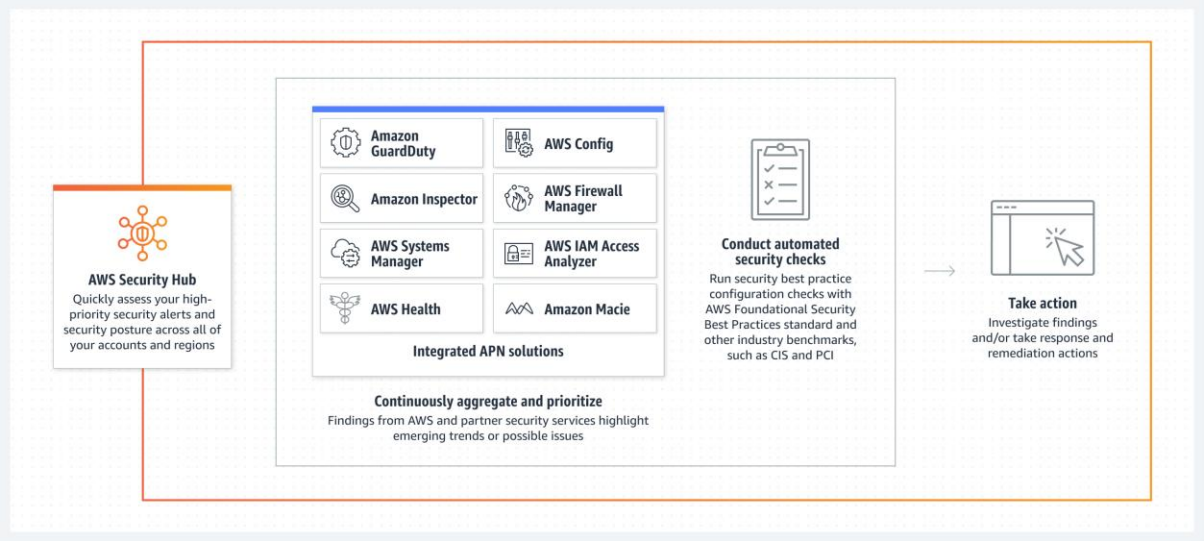
Relevant security news and updates are communicated on a weekly basis to employees through different channels (e.g., meetings, email, intranet) to promote organization-wide awareness and engagement in cybersecurity practices.

Additionally, the ISO notifies relevant teams when software or system updates are released and ensures that security patches and updates are applied in a timely manner.

b. Vulnerability Scans

AWS Security Hub provides a comprehensive view of the organization's security posture within the AWS environment and enables continuous assessment against recognized industry standards. It aggregates findings from native AWS services such as Amazon GuardDuty, Amazon Inspector, and Amazon CloudWatch, while also performing its own continuous automated security checks.

Security Hub automatically prioritizes findings based on severity and uses predefined insights to highlight recurring or systemic security issues requiring remediation. Automatic notifications for Critical and High vulnerabilities are configured through AWS Simple Notification Service (SNS) to alert the CISO, Information Security Officer (ISO), and ISMS Manager.



Supplier Shield™ conducts weekly automated penetration tests on the following domains to proactively identify and address vulnerabilities:

- suppliershield.com
- app.suppliershield.com
- dev-app.suppliershield.com
- dev.suppliershield.com
- stg.suppliershield.com
- staging-app.suppliershield.com

Findings from automated vulnerability scans are reviewed, prioritized, and addressed in accordance with the Change Management Policy and defined vulnerability remediation targets, ensuring timely correction, controlled implementation, and verification of effectiveness prior to deployment.

c. Testing, Security Review and Access Control Activities

- **Unit tests** are performed by the Quality Assurance (QA) team on all new or modified features to verify their proper functionality and compliance with development standards.
- **Transversal tests** are executed by the QA team when deploying a development release to the staging environment, to validate integration between components and detect cross-functional defects.
- **User Acceptance Testing** is conducted by the Supplier Shield users, the Product Development Director, and Management to ensure that the delivered functionalities meet business and operational requirements prior to production release.
- **Manual penetration tests** are performed for each major release and at least twice per year. Summaries of penetration test results are made available to stakeholders through the Supplier Shield™ Trust Centre, supporting transparency and continuous improvement of the platform's security posture.
- **Automated security reviews** are conducted on all third-party libraries and dependencies used within the development environment to detect and remediate known vulnerabilities.
- **Peer code reviews** are mandatory for all software developments and must be performed through a pull-request process prior to code integration into the main branch.
- **Least privilege principle** in the provision of accesses to all environments.
- **AI-assisted tools** may be used if their outputs are reviewed and validated by the developer before implementation and if operated in a secure, isolated environment where data is not reused or retained for training external AI models.

d. Vulnerability Remediation Targets

Systems must be updated with relevant security patches within the following defined time frame:

CVSS score	Internet-facing assets	Internal assets
9.0 to 10	Target remediation days: 1	Target remediation days: 2
7.0 to 8.9	Target remediation days: 5	Target remediation days: 5
4.0 to 6.9	Target remediation days: 10	Target remediation days: 30
0.0 to 3.9	Target remediation days: routine maintenance tasks	Target remediation days: routine maintenance tasks

6. Document Control

a. Approval

This version is validated as of 01.11.2025 and supersedes all previous versions. For further information, please contact us via email: request@suppliershield.ch.

Title	**Vulnerability Management Policy**
Approved By	Alexis Hirschhorn
Date of Approval	01.10.2025
Version Number	1.1

b. Version History

Version	Date	Reason for Amendment
1.0	02.09.2023	Initial version
1.0	05.10.2024	Review (no change)
1.1	01.10.2025	Review and update purpose, scope, roles & responsibilities, vulnerability management controls