



Coordinated Vulnerability Disclosure Policy

Version: 1.0

Effective from: 11.09.2026

Last updated: 11.09.2026

Table of Contents

1	Purpose	2
2	Scope.....	2
3	Contact Options	2
4	Which Reports Should Be Submitted?	3
5	What Information Should a Report Contain?	3
6	Valid Reports	3
7	Communication Requirements	3
8	Assurances by the SITS Group	4
9	Response Times	4
10	Disclosure of Vulnerabilities	4
11	End of the CVD Process	5

1 Purpose

The security of our products is a top priority for the SITS Group. Despite appropriate security measures, vulnerabilities and security incidents cannot be completely ruled out. This Policy describes how potential vulnerabilities, indications of actively exploited vulnerabilities, and other security-relevant incidents can be reported, assessed, addressed and, where appropriate, disclosed.

Our aim is to work collaboratively and on a basis of trust with security researchers, customers, partners and other reporters in order to identify, assess and remediate security risks quickly and responsibly.

2 Scope

This Policy applies to products with digital elements that are developed or manufactured by Swiss IT Security AG or SITS Deutschland GmbH and made available on the market under the name or trademark of the respective responsible company. Vulnerability reports are received, assessed and addressed centrally by the Product Security Incident Response Team (PSIRT) of the SITS Group.

This Policy does not cover:

- general support requests
- product requests
- vulnerabilities in third-party products for which neither Swiss IT Security AG nor SITS Deutschland GmbH is responsible as the manufacturer

3 Contact Options

Reports can be submitted through the following channels:

1.) PSIRT

Email: psirt@sits.com

The PSIRT is responsible for receiving, assessing and addressing reports.

2.) Web Form

In addition, a web form for reporting vulnerabilities and security incidents is available on the SITS Group website.

Preferred Languages

Reports may be submitted in German or English. Communication will preferably be conducted in German or English.

4 Which Reports Should Be Submitted?

We welcome reports concerning (actively exploited) vulnerabilities and security-relevant incidents relating to products within the scope of this Policy, in particular:

- security flaws
- vulnerabilities affecting confidentiality, integrity or availability
- indications of actively exploited vulnerabilities
- security-relevant incidents
- other security-relevant observations

5 What Information Should a Report Contain?

For efficient processing, we recommend providing the following information, where available:

- affected product
- affected version
- description of the vulnerability or security incident
- technical impact
- steps to reproduce
- screenshots
- log files
- risk assessment

The more complete the information provided, the faster the analysis can be carried out.

6 Valid Reports

A report is generally considered valid if:

- it concerns a product covered by this Policy
- sufficient information is provided for an assessment
- an actual vulnerability or security issue is described

Automated scan results without an adequate technical description or verifiable evidence may be rejected.

7 Communication Requirements

The SITS Group expects all parties involved to interact respectfully and professionally. Discrimination, insults, harassment or other inappropriate conduct will not be tolerated.

All incoming reports will be reviewed in accordance with the four-eyes principle or with the involvement of additional qualified persons, where organisationally possible. Reports will not be rejected solely on the basis of an individual decision.

8 Assurances by the SITS Group

The SITS Group undertakes to:

- treat every incoming report confidentially to the extent permitted by law
- not disclose the reporter's personal data to third parties without the reporter's express consent
- respond to incoming reports within the response times defined in this Policy
- remain available as the point of contact for a trust-based exchange throughout the entire processing procedure
- not require a non-disclosure agreement (NDA) for reporting a vulnerability or security incident
- not take legal action against reporters provided that they act in good faith, comply with this Policy, and there is no evident criminal or abusive intent

9 Response Times

Initial Response

A personal acknowledgement of receipt of the report will be provided within five working days.

Detailed Feedback

Within ten working days, the reporter will receive feedback containing at least one of the following elements:

- a statement by the SITS Group confirming or denying the existence of the reported vulnerability or security incident
- follow-up questions to better understand the report
- an explanation of why the investigation requires more time, together with a commitment to provide a status update within ten working days

10 Disclosure of Vulnerabilities

Validated and verified vulnerabilities will generally be disclosed to users within 90 days of their confirmation. Disclosure may be omitted if the respective responsible manufacturing company becomes aware of a vulnerability and fully remediates it before the affected product is placed on the market.

Where there is an objective justification for delaying the remediation or mitigation of a vulnerability, the disclosure period may, in close coordination with the competent national Computer Security Incident Response Team (CSIRT), be extended once by a further 90 days. In exceptional cases, the period may

be further extended by the competent national CSIRT at the request of the respective responsible manufacturing company.

Disclosure will be carried out by the respective responsible manufacturing company and in coordination with the competent national CSIRT or the European Union Agency for Cybersecurity (ENISA).

Regulatory Reports

Where the legal requirements are met, the respective responsible manufacturing company will report actively exploited vulnerabilities and severe security incidents relating to products covered by this Policy to the competent bodies in accordance with the applicable regulatory requirements, in particular to ENISA and the competent CSIRT.

11 End of the CVD Process

A CVD case is generally considered closed if

- the information provided in the vulnerability report proves to be unfounded
- the vulnerability in a product has been fixed and disclosed to users
- the vulnerability has been mitigated or fixed by means of an appropriate patch or other appropriate measures and disclosed to users

In addition, the SITS Group may consider the CVD process closed if:

- the reporter does not respond to technical or substantive follow-up questions for at least 30 days and, as a result, the report can only be processed to a limited extent or cannot be processed further
- the vulnerability has been disclosed to users and, in coordination with the competent national CSIRT, it can no longer be assumed that further mitigation or fix will take place

The SITS Group will inform the reporter that the case has been closed.