

Coordinated Vulnerability Disclosure Policy

Version: 1.0

Gültig ab: 11.09.2026

Letzte Aktualisierung: 11.09.2026

Inhaltsverzeichnis

1	Zweck	2
2	Geltungsbereich.....	2
3	Kontaktmöglichkeiten	2
4	Welche Meldungen sollen eingereicht werden?	3
5	Welche Informationen sollte eine Meldung enthalten?	3
6	Gültige Meldungen	3
7	Anforderungen an die Kommunikation	4
8	Zusicherungen der SITS Group.....	4
9	Reaktionszeiten	4
10	Offenlegung von Schwachstellen	5
11	Abschluss des CVD-Prozesses.....	5

1 Zweck

Die Sicherheit unserer Produkte hat für die SITS Group höchste Priorität. Trotz angemessener Sicherheitsmaßnahmen können Schwachstellen und Sicherheitsvorfälle nicht vollständig ausgeschlossen werden. Diese Richtlinie beschreibt, wie potenzielle Schwachstellen, Hinweise auf aktiv ausgenutzte Schwachstellen sowie sonstige sicherheitsrelevante Vorfälle gemeldet, bewertet, behandelt und gegebenenfalls veröffentlicht werden.

Unser Ziel ist eine vertrauensvolle Zusammenarbeit mit Sicherheitsforschern, Kunden, Partnern und anderen Meldenden, um Sicherheitsrisiken schnell und verantwortungsvoll zu identifizieren, zu bewerten und zu beheben.

2 Geltungsbereich

Diese Richtlinie gilt für Produkte mit digitalen Elementen, die von der Swiss IT Security AG oder der SITS Deutschland GmbH entwickelt oder hergestellt und unter dem Namen oder der Marke der jeweils verantwortlichen Gesellschaft auf dem Markt bereitgestellt werden. Die Entgegennahme, Bewertung und Behandlung von Schwachstellenmeldungen erfolgt zentral über das Product Security Incident Response Team (PSIRT) der SITS Group.

Nicht unter diese Richtlinie fallen:

- allgemeine Supportanfragen
- Produktwünsche
- Schwachstellen in Produkten Dritter, für welche weder die Swiss IT Security AG noch die SITS Deutschland GmbH als Hersteller verantwortlich sind

3 Kontaktmöglichkeiten

Meldungen können über nachstehende Kanäle eingereicht werden:

1.) PSIRT

E-Mail: psirt@sits.com

Das PSIRT ist verantwortlich für die Entgegennahme, Bewertung und Behandlung von Meldungen.

2.) Webformular

Zusätzlich steht auf der Website der SITS Group ein Webformular für Schwachstellenmeldungen und Sicherheitsvorfälle zur Verfügung.

Bevorzugte Sprachen

Meldungen können in deutscher oder englischer Sprache eingereicht werden. Die Kommunikation erfolgt vorzugsweise in deutscher oder englischer Sprache.

4 Welche Meldungen sollen eingereicht werden?

Wir begrüßen Meldungen zu (aktiv ausgenutzten) Schwachstellen und sicherheitsrelevanten Vorfällen mit Bezug zu Produkten, die unter den Geltungsbereich dieser Richtlinie fallen, insbesondere:

- Sicherheitslücken
- Schwachstellen mit Auswirkungen auf Vertraulichkeit, Integrität oder Verfügbarkeit
- Hinweise auf aktiv ausgenutzte Schwachstellen
- sicherheitsrelevante Vorfälle
- sonstige sicherheitsrelevante Beobachtungen

5 Welche Informationen sollte eine Meldung enthalten?

Für eine effiziente Bearbeitung empfehlen wir die Übermittlung folgender Informationen (falls vorhanden):

- betroffenes Produkt
- betroffene Version
- Beschreibung der Schwachstelle oder des Sicherheitsvorfalls
- technische Auswirkungen
- Schritte zur Reproduktion
- Screenshots
- Logfiles
- Risikoeinschätzung

Je vollständiger die bereitgestellten Informationen sind, desto schneller kann die Analyse erfolgen.

6 Gültige Meldungen

Eine Meldung gilt grundsätzlich als valide, wenn:

- sie ein von dieser Richtlinie erfasstes Produkt betrifft
- ausreichend Informationen für eine Bewertung bereitgestellt werden
- tatsächlich eine Schwachstelle oder ein Sicherheitsproblem beschrieben wird

Automatisierte Scannergebnisse ohne ausreichende technische Beschreibung oder nachvollziehbare Nachweise können zurückgewiesen werden.

7 Anforderungen an die Kommunikation

Die SITS Group erwartet von allen Beteiligten einen respektvollen und professionellen Umgang. Diskriminierung, Beleidigungen, Belästigungen oder andere unangemessene Verhaltensweisen werden nicht toleriert.

Alle eingehenden Meldungen werden nach dem Vier-Augen-Prinzip bzw. unter Einbezug weiterer qualifizierter Personen geprüft, soweit dies organisatorisch möglich ist. Meldungen werden nicht allein aufgrund einer Einzelentscheidung verworfen.

8 Zusicherungen der SITS Group

Die SITS Group verpflichtet sich:

- jede eingehende Meldung vertraulich zu behandeln, soweit dies rechtlich zulässig ist
- personenbezogene Daten des Meldenden nicht ohne dessen ausdrückliche Zustimmung an Dritte weiterzugeben
- innerhalb der in dieser Richtlinie definierten Reaktionszeiten auf eingehende Meldungen zu reagieren
- während des gesamten Bearbeitungsprozesses als Ansprechpartner für einen vertrauensvollen Austausch zur Verfügung zu stehen
- keine Geheimhaltungsvereinbarung (NDA) für die Meldung einer Schwachstelle oder eines Sicherheitsvorfalls zu verlangen
- keine rechtlichen Schritte gegen Meldende einzuleiten, sofern diese in gutem Glauben handeln, diese Richtlinie einhalten und keine erkennbar strafbare oder missbräuchliche Absicht vorliegt

9 Reaktionszeiten

Erste einfache Antwort

Innerhalb von fünf Arbeitstagen erfolgt eine persönliche Bestätigung des Eingangs der Meldung.

Detailliertes Feedback

Innerhalb von zehn Arbeitstagen erhält die meldende Person ein Feedback, welches mindestens eines der folgenden Elemente enthält:

- eine Stellungnahme der SITS Group, in der diese bestätigt oder dementiert, dass die gemeldete Schwachstelle bzw. der gemeldete Sicherheitsvorfall vorliegt
- Rückfragen zum besseren Verständnis der Meldung
- eine Erklärung, weshalb die Untersuchung mehr Zeit benötigt, zusammen mit der Zusage, innerhalb von zehn Arbeitstagen einen aktuellen Stand mitzuteilen

10 Offenlegung von Schwachstellen

Validierte und verifizierte Schwachstellen werden grundsätzlich innerhalb von 90 Tagen nach ihrer Bestätigung den Nutzern offengelegt. Die Offenlegung kann entfallen, wenn die jeweils verantwortliche Herstellergesellschaft von einer Schwachstelle Kenntnis erlangt und diese vollständig behebt, bevor das betroffene Produkt auf den Markt gebracht wird.

Liegt eine sachliche Begründung für eine Verzögerung der Behebung oder Mitigation einer Schwachstelle vor, kann die Frist bis zur Offenlegung in enger Abstimmung mit dem zuständigen nationalen Computer Security Incident Response Team (CSIRT) einmalig um weitere 90 Tage verlängert werden. In Ausnahmefällen kann die Frist auf Antrag der jeweils verantwortlichen Herstellergesellschaft durch das zuständige nationale CSIRT weiter verlängert werden.

Die Offenlegung erfolgt durch die jeweils verantwortliche Herstellergesellschaft und in Abstimmung mit dem zuständigen nationalen CSIRT oder der Agentur der Europäischen Union für Cybersicherheit (ENISA).

Regulatorische Meldungen

Sofern die gesetzlichen Voraussetzungen erfüllt sind, meldet die jeweils verantwortliche Herstellergesellschaft aktiv ausgenutzte Schwachstellen sowie schwerwiegende Sicherheitsvorfälle im Zusammenhang mit den von dieser Richtlinie erfassten Produkten gemäss den anwendbaren regulatorischen Anforderungen an die zuständigen Stellen, insbesondere an die ENISA und zuständige CSIRT.

11 Abschluss des CVD-Prozesses

Ein CVD-Fall gilt grundsätzlich als abgeschlossen, wenn

- sich die Hinweise aus der Schwachstellenmeldung als unbegründet herausstellen
- die Schwachstelle eines Produkts behoben wurde und den Nutzern offengelegt wurde
- die Schwachstelle durch einen geeigneten Patch oder andere geeignete Massnahmen mitigiert oder behoben wurde und den Nutzern offengelegt wurde

Darüber hinaus kann die SITS Group den CVD-Prozess als abgeschlossen betrachten, wenn:

- die meldende Person während mindestens 30 Tagen nicht auf technische oder inhaltliche Rückfragen reagiert und die Meldung deshalb nur eingeschränkt oder nicht weiterbearbeitet werden kann

- die Schwachstelle den Nutzern offengelegt wurde und in Abstimmung mit dem zuständigen nationalen CSIRT nicht mehr davon ausgegangen werden kann, dass eine weitere Mitigation oder Behebung erfolgt

Die SITS Group informiert die meldende Person über den Abschluss des Vorgangs.