HAPA

a coesia company

Coordinated Vulnerability Disclosure Policy

Coordinated Vulnerability Disclosure Policy

Index

Date of release: 11/09/2026

1. Purpose

Hapa AG maintains a Coordinated Vulnerability Disclosure Policy to enable responsible reporting and remediation of security vulnerabilities affecting products with digital elements. This policy supports compliance with Regulation (EU) 2024/2847. Reported vulnerabilities will be handled in accordance with applicable legal and regulatory requirements.

2. Scope

This Policy applies to all Hapa AG products with digital elements and related software components falling within the scope of Regulation (EU) 2024/2847.

3. How to Report

Vulnerabilities may be reported via:

- Email: security@hapa.ch
- Postal address: Hapa AG, PSIRT, Chriesbaumstrasse 4, CH-8604 Volketswil
- Form accessible with the “Report a cyber incident” button on our website (www.hapa.ch).

4. Required Report Information

A vulnerability report must contain at least the following information:

- Affected product (including the machine serial number, if available)
- Affected version
- Vulnerability description
- Reproduction information if available
- Reporter’s contact details

5. Coordinated Vulnerability Disclosure Process

Upon receipt of a vulnerability report, Hapa AG will:

- acknowledge receipt of the report within seven calendar days
- review and validate the reported vulnerability
- maintain reasonable communication with the reporter throughout the assessment process
- coordinate the timing and content of any public disclosure with the reporter whenever appropriate
- where required by Regulation (EU) 2024/2847, report actively exploited vulnerabilities and severe incidents to the competent authorities and ENISA.

The Hapa AG Product Security Incident Response Team (PSIRT) is responsible for intake, assessment, remediation coordination, disclosure decisions and CRA reporting.

6. Good Faith Research / Safe Harbor

Hapa AG values collaboration with security researchers and users in identifying and responsibly disclosing vulnerabilities.
Security testing is permitted only to the extent necessary to identify and demonstrate a vulnerability, provided such testing does not adversely affect systems, data, or users.

It is forbidden to

- Access, modify or extract personal, confidential or sensitive data from the system not necessary to report a vulnerability.
- Compromise service availability on the system being analyzed (e.g., through denial-of-service attacks).
- Introduce malware into the system being analyzed.
- Copy, modify, or delete data in the system being analyzed.
- Make changes to the system being analyzed.

- Perform excessive or unauthorized access attempts or share login credentials with third parties.
- Execute brute force attacks to gain access to a system.
- Exploit the vulnerability for purposes other than reporting.
- Publicly disclose the vulnerability without Hapa AG's prior written authorization.

Hapa AG will not pursue legal action against persons acting in good faith and in compliance with this policy.

7. Disclosure and Recognition

Hapa AG may publicly acknowledge reporters who contribute valid vulnerability reports, subject to their consent.

8. Privacy

Personal data provided in vulnerability reports will be processed solely for the purpose of vulnerability handling and in accordance with applicable data protection laws.

9. Version Maintenance

This policy may be updated from time to time. The current version is published on the Hapa AG website.