# Vulnerability Disclosure Policy (VDP)

## 1. Purpose

Waystream is committed to designing, developing and maintaining secure networking products throughout their supported lifecycle.

We welcome responsible vulnerability reports from customers, security researchers, partners and other stakeholders. Responsible disclosure helps improve the security of our products and reduce potential risks to our customers.

This Vulnerability Disclosure Policy explains how security vulnerabilities affecting Waystream products can be reported, how reports are handled and how security information may be communicated.

Waystream's Product Security Program is based on internationally recognised practices for Coordinated Vulnerability Disclosure (CVD) and supports applicable regulatory requirements, including the EU Cyber Resilience Act (CRA).

## 2. Scope

This policy applies to security vulnerabilities that may affect supported Waystream products, including access switches and optical transceiver modules.

This policy does not normally apply to:

- general technical support requests, including questions or issues related solely to customer network configuration
- feature requests or product enhancements
- products that have reached End-of-Support, which may instead be assessed on a case-by-case basis.

A security issue involving a Waystream product is not excluded merely because a particular configuration or deployment is required to trigger or expose the vulnerability.

Reports outside the scope of this policy may be redirected to another appropriate Waystream function.

## 3. Reporting a Vulnerability

If you believe you have identified a security vulnerability affecting a Waystream product, we encourage you to report it to Waystream's Product Security Incident Response Team.

E-mail: security@waystream.com

Waystream supports encrypted communication using PGP. The current public key is available in the product security section at waystream.com (waystream.com/en/services-support/security/)

Reports may also be submitted anonymously. Where appropriate, vulnerabilities may additionally be reported, by Waystream, through the Single Reporting Platform by ENISA and/or relevant national CSIRT in accordance with regulatory requirements.

## 4. Information to Include

Providing detailed technical information helps us investigate reports efficiently.

Where possible, please include:

- product name
- hardware revision
- firmware version
- vulnerability description
- steps required to reproduce the issue
- expected behaviour
- observed behaviour
- core files (if available)
- screenshots, logs or packet captures (if available)
- proof-of-concept information (if available)
- known mitigations (optional)
- your contact details (optional)
- show tech support (optional)

Please avoid including customer-confidential information unless specifically requested through an agreed secure communication channel.

Incomplete reports are welcome if sufficient information is available to begin an investigation.

## 5. What Happens Next

After receiving a report, Waystream aims to:

- acknowledge receipt of the report;
- review the submitted information;
- validate the reported vulnerability;

- assess potential customer impact and severity;
- determine whether supported products are affected;
- assess available remediation or mitigation options;
- coordinate disclosure activities where appropriate; and
- communicate relevant security information to customers when necessary.

During the investigation, Waystream may request additional technical information from the reporter.

## 6. Response Objectives

Waystream aims to process vulnerability reports as promptly as reasonably possible and in accordance with applicable regulatory requirements, including the Cyber Resilience Act (CRA)

Our normal response objectives are:

| **Activity** | **Objective** |
|---|---|
| Initial acknowledgement | Normally within two business days |
| Initial technical review | As soon as reasonably practicable |
| Status updates | Where appropriate during the investigation |
| Public communication | When appropriate mitigation or remediation information is available |

These objectives represent operational targets rather than contractual service commitments and may vary depending on the complexity, severity and quality of the reported information.

Where a reported vulnerability or security incident triggers mandatory reporting obligations under the CRA, Waystream will follow the applicable regulatory reporting requirements and deadlines.

## 7. Coordinated Vulnerability Disclosure

Waystream supports responsible and coordinated vulnerability disclosure.

We encourage reporters to allow reasonable time for investigation and remediation before publicly disclosing technical details.

Where appropriate, Waystream may coordinate disclosure activities with:

- the reporter
- component suppliers
- CERT/CSIRT organisations

- relevant authorities
- CVE Numbering Authorities (CNAs)
- other affected parties

Where necessary to protect customers or comply with applicable legal obligations, Waystream may disclose vulnerability information earlier than originally planned.

## 8. Product Security Advisories

Where customer awareness or corrective action is considered necessary, Waystream may publish a Product Security Advisory.

A typical advisory may include:

- Advisory ID
- publication date
- severity
- affected products
- affected firmware versions
- CVE reference (where applicable)
- CVSS score
- vulnerability description
- available mitigations
- fixed firmware versions
- upgrade recommendations

Where applicable, firmware updates and supporting documentation are made available through the Waystream Customer Portal.

## 9. CVE Coordination

Where appropriate, Waystream may request or coordinate assignment of a Common Vulnerabilities and Exposures (CVE) identifier.

Not every confirmed vulnerability will necessarily receive a CVE identifier.

## 10. Safe Harbor

Waystream supports legitimate security research performed responsibly and in good faith.

Waystream does not intend to pursue legal action against individuals who, while acting in good faith and in accordance with this policy and applicable law:

- make reasonable efforts to avoid harm;
- avoid unnecessary disruption of products or services;
- avoid accessing, modifying or disclosing customer information;
- avoid social engineering;
- avoid denial-of-service testing;
- avoid physical attacks;
- avoid establishing persistent access;
- avoid testing customer production networks without explicit authorization; and
- provide reasonable opportunity for coordinated vulnerability disclosure.

This statement does not limit the rights of customers, third parties or competent authorities.

## 11. Recognition

Subject to the reporter's consent and where appropriate, Waystream may acknowledge individuals or organisations that responsibly report validated security vulnerabilities.

## 12. Supported Products

This policy primarily applies to products that remain within their published support lifecycle.

For products that have reached End-of-Support, Waystream may assess reported vulnerabilities on a case-by-case basis, taking into account factors such as:

- customer impact
- severity
- active exploitation
- technical feasibility
- applicable legal or regulatory obligations

## 13. Privacy

Personal information submitted together with vulnerability reports is processed only for the purpose of receiving, investigating and managing the reported vulnerability.

Information may be shared internally or, where necessary, with suppliers, competent authorities or other relevant parties involved in coordinated vulnerability handling.

Waystream will seek to avoid unnecessary disclosure of the reporter's identity unless required by law or agreed with the reporter.

## 14. Policy Updates

Waystream may revise this policy from time to time to reflect changes in products, processes, standards or legal requirements.

The latest version will always be available from the Product Security section of the Waystream website.

## 15. Contact

**Email**
security@waystream.com

**Product Security information**
waystream.com/en/services-support/security/