Responsible Vulnerability Disclosure Policy

Last Reviewed	@November 11, 2025
Created By	Ⓑ Blake Ryan
Confidentiality Level	TLP:GREEN
Last Review	@November 11, 2025
Due For Review	@November 11, 2026

Revision Date	Version	Created By	Description of change
11/11/2025	1.0	Blake Ryan	Basic document outline
11/14/2025	1.1	Blake Ryan	Draft Submitted for Review
11/15/2025	1.2	Juan Lagares	Draft Document Approved

Table of Contents

Responsible Vulnerability Disclosure Policy

WaveStar Solutions

1 Purpose

WaveStar Solutions is committed to maintaining the security and integrity of its products, services, and infrastructure. This **Responsible Vulnerability Disclosure Policy** establishes a clear process for external individuals, customers, and partners to report potential vulnerabilities or security risks in a responsible and coordinated manner.

The purpose of this policy is to protect WaveStar's clients, partners, and systems while encouraging open collaboration with the security community.

For security-related inquiries or to report a vulnerability, contact:

security@wavestarsolutions.com

2 Objectives

This policy aims to:

- Provide a transparent process for identifying and responsibly disclosing vulnerabilities.
- Protect sensitive and customer data from unauthorized exposure.
- Promote cooperation between WaveStar and external researchers, customers, or partners.
- Ensure vulnerabilities are remediated quickly and safely.

- Align with applicable regulatory and contractual obligations, including those specific to telecommunications and data protection standards.

3 Scope

This policy applies to:

- All **WaveStar Solutions systems, services, networks, and applications**.
- Vulnerabilities or exposures identified in any environment under WaveStar's operational control.
- Reports submitted by external researchers, customers, partners, or members of the public.
- Incidents involving confidential, proprietary, or customer-related data.

4 Principles of Responsible Disclosure

WaveStar Solutions encourages good-faith research and coordinated disclosure. Reporters are expected to follow these principles:

- **Good Faith Reporting:** Submit findings responsibly, without intent to harm, disrupt, or exploit.
- **No Unauthorized Testing:** Avoid activities that could impact systems, services, or customer data.
- **Confidentiality:** Do not publicly share details until WaveStar confirms resolution.
- **Safe Harbor:** Researchers who comply with this policy will not face legal action or account restrictions as a result of their responsible disclosure.

5 Reporting a Vulnerability

5.1 How to Report

To report a security issue or potential vulnerability, email:

security@wavestarsolutions.com

Include the following details when submitting a report:

- Description of the issue and affected system or service.
- Steps to reproduce or validate the finding.
- Supporting materials such as screenshots, logs, or proof-of-concept code (if safe to share).
- Contact information for coordination and follow-up.

5.2 Do Not Include

Reporters must **not** share:

- Personally identifiable information (PII) or customer data.
- Confidential or proprietary data obtained during testing.
- Any information that could enable others to exploit the issue before it is resolved.

---

6 WaveStar's Response Process

WaveStar Solutions follows a consistent process for reviewing and addressing vulnerability reports:

1. **Acknowledgment:** The Information Security Team acknowledges receipt of a report within **5 business days**.
2. **Assessment:** The issue is verified, classified by severity, and logged in WaveStar's tracking system.
3. **Remediation:** Appropriate teams implement fixes or mitigations based on risk level.
4. **Coordination:** The reporter may be contacted for additional details or verification.
5. **Disclosure:** After resolution, WaveStar may publish an advisory summarizing the issue and corrective action, coordinated with the reporter.

---

7 Handling of Sensitive or Proprietary Information

- Confidential or restricted information must not be shared externally without executive authorization.
- When disclosure is legally or contractually required, it must follow established approval workflows.
- Sensitive data shared with authorized parties must be encrypted, logged, and labeled with confidentiality notices.
- Public statements regarding vulnerabilities or incidents must be cleared through Corporate Communications and Legal.

---

8 Third-Party and Customer Data

If a reported issue involves third-party or customer data, WaveStar will:

- Notify the affected entity promptly as required by contract or regulation.
- Coordinate with all parties to verify impact and remediation.
- Delay any public disclosure until all affected stakeholders agree.

---

9 Breach and Notification Procedures

In the event of a confirmed breach or unauthorized disclosure:

- The incident will be investigated and contained according to the **Incident Response Plan**.
- Affected customers, partners, or regulators will be notified **without undue delay**, consistent with applicable laws and contractual terms.
- Notifications will include a description of the event, corrective measures, and recommended next steps.

---

10 Record-Keeping and Transparency

WaveStar maintains records of all reported vulnerabilities and disclosure events, including:

- Dates of receipt, verification, and resolution.

- Communications with reporters and affected entities.
- Actions taken and lessons learned.

Records are reviewed annually to support continuous improvement and compliance verification.

11 Compliance and Enforcement

Failure to comply with this policy may result in disciplinary action, including termination or contract suspension.

Unauthorized data disclosure, exploitation of vulnerabilities, or unapproved testing may result in legal action.

12 Monitoring and Review

This policy shall be reviewed at least **annually**, or sooner if significant system, regulatory, or operational changes occur.

The **Chief Executive Officer (CEO)** of WaveStar Solutions is the owner of this document and must approve any updates. The **Information Security Team** is responsible for daily oversight and management of vulnerability reports.