BILERRO Coordinated Vulnerability Disclosure Policy (CVD)

Paseo Miramón, 170 – 20014 Donostia (Gipuzkoa), España

VERSION CONTROL

Version	Date	Responsible	Comments
v1.0	11/09/2026	Asier Martinez Juanaberria	Initial version

CONTENTS

1 Purpose

BILERRO is committed to maintaining the security, integrity, and resilience of its products and services. This Coordinated Vulnerability Disclosure (CVD) Policy establishes a formal process for receiving, assessing, remediating, and disclosing security vulnerabilities in a responsible manner.

The objectives of this policy are to:

- Enable security researchers, customers, partners, and third parties to report vulnerabilities securely.
- Facilitate the timely assessment and remediation of reported vulnerabilities.
- Minimize potential risks to customers and affected stakeholders.
- Promote responsible disclosure practices.
- Support BILERRO's cybersecurity and vulnerability management obligations.

2 Scope

This policy applies to all products, software, services, and digital components developed, maintained, or distributed by BILERRO, and any future products and services placed under BILERRO's responsibility.

3 Reporting a Vulnerability

Security vulnerabilities should be reported to:

Email: security@bilerro.com

To facilitate efficient assessment, reports should include, where possible:

- Affected product.
- Hardware version.
- Software/Firmware version.
- Affected project, deployment, or contract reference.
- Affected train series, fleets or individual units.
- A clear description of the vulnerability.
- Technical details sufficient to reproduce the issue.
- Potential security impact.
- Proof-of-concept information, if available.
- Any proposed mitigation measures.
- Contact information for follow-up communication.

Incomplete reports may still be reviewed if sufficient information is provided to identify the issue.

4 Secure Communications

Reporters are encouraged to encrypt their communications using BILERRO's OpenPGP public key.

OpenPGP Public Key: https://www.bilerro.com/security/bilerro-security-team-gpg.asc

4.1 Security.txt

To facilitate the responsible reporting of security vulnerabilities, BILERRO publishes a security.txt file in accordance with industry best practices.

The security.txt file provides researchers, customers, partners, and other stakeholders with authoritative security contact information and references to relevant security resources.

The file is published at: https://www.bilerro.com/.well-known/security.txt

The security.txt file may include:

- Security contact information.
- OpenPGP public key location.
- Vulnerability Disclosure Policy reference.
- Supported languages.
- Expiration date of the published information.
- Additional security-related references deemed relevant by BILERRO.

BILERRO will maintain the information contained in the security.txt file accurate and up to date. Any changes to security contact information or disclosure procedures shall be reflected in the published security.txt file without undue delay.

Researchers and other stakeholders are encouraged to consult the security.txt file before reporting security vulnerabilities.

5 Response Process

Upon receipt of a vulnerability report, BILERRO will perform the following activities:

5.1 Acknowledgement

BILERRO will acknowledge receipt of the report within three (3) business days.

5.2 5.2 Initial Assessment

An initial review will be performed within ten (10) business days to determine:

- Whether the reported issue constitutes a security vulnerability.
- The potentially affected products or services.
- The likely impact and severity.

5.3 Validation

If the issue is confirmed, BILERRO will:

- Register the vulnerability within its vulnerability management process.
- Assign a severity rating based on risk and exploitability.
- Define remediation and containment actions.
- Track remediation activities through closure.

5.4 Communication

BILERRO will maintain reasonable communication with the reporter regarding:

- Report status.
- Validation outcome.
- Remediation progress.
- Planned public disclosure, where applicable.

6 Coordinated Disclosure Principles

BILERRO supports responsible and coordinated disclosure.

Reporters are requested to:

- Avoid public disclosure before remediation or mitigation measures are available.
- Allow BILERRO a reasonable period to investigate and address the reported issue.
- Refrain from actions that could unnecessarily increase risk to customers, infrastructure, or third parties.

BILERRO will make reasonable efforts to develop and distribute corrective measures as quickly as practicable, considering the severity and complexity of the vulnerability.

7 Security Advisories

Where appropriate, BILERRO may publish Security Advisories containing:

- Vulnerability identifier.
- Affected products and versions.
- Severity classification.
- Description of the issue.
- Impact assessment.
- Mitigation measures.
- Remediation instructions.
- Availability of fixes or updates.
- Acknowledgement of the reporter, with prior consent.

8 Authorized Research Activities

BILERRO welcomes good-faith security research conducted in a responsible manner.

Researchers should:

- Avoid disruption of production environments.
- Avoid unauthorized access to customer data.
- Avoid data modification, destruction, or exfiltration.
- Avoid denial-of-service testing.
- Limit testing to the minimum necessary to demonstrate the vulnerability.

Activities that could impact safety, operational continuity, regulatory compliance, or customer confidentiality are strictly prohibited.

9 Safe Harbor Statement

BILERRO will not pursue legal action against individuals who:

- Act in good faith.
- Comply with this policy.
- Avoid causing harm to customers, systems, or data.
- Promptly report discovered vulnerabilities through the designated channels.

This Safe Harbor provision does not apply to activities that violate applicable laws or regulations.

10 Vulnerability Handling and Remediation

Confirmed vulnerabilities will be managed through BILERRO's vulnerability management process, including:

- Risk assessment.
- Root cause analysis.
- Corrective action planning.
- Security testing and validation.
- Deployment of remediation measures.
- Customer notification where appropriate.

Remediation priorities shall be determined according to the severity of the vulnerability and its potential impact on confidentiality, integrity, availability, safety, and operational continuity.

11 Confidentiality

Information relating to reported vulnerabilities will be handled on a need-to-know basis and protected in accordance with BILERRO's information security requirements.

BILERRO expects reporters to maintain confidentiality until coordinated disclosure has been agreed.

12 Policy Review

This policy shall be reviewed at least annually, or earlier if required by:

- Regulatory changes.
- Significant security incidents.
- Changes to BILERRO's products or services.
- Improvements identified through operational experience.