MODIFICATION SUMMARY

Revision	Changes Summary	Written by	Verified by	Approved by	Date
A	Creation	C. Mace			

Table of Contents

1. Introduction and Purpose

Our company is committed to maintaining a robust security environment for our customers and users. We recognize the importance of responsible and transparent collaboration with the information security community to identify and resolve vulnerabilities effectively.

This policy establishes a coordinated disclosure framework that allows security researchers to contact us and report vulnerabilities responsibly, while protecting our users and maintaining the confidentiality of sensitive information.

As part of this coordinated disclosure, the initial report is first made privately to the company and made public after a period specified in this document, in a coordinated communication with the researcher(s) who reported the vulnerability.

2. Definitions

Vulnerability: A weakness in our systems, applications, or processes that could be exploited to compromise the confidentiality, integrity, or availability of data or services.

Security Researcher: Any person or organization that discovers and reports a vulnerability responsibly.

Coordinated Disclosure: A process whereby the researcher reports the vulnerability to our team, which has a defined period to develop and deploy a fix before public disclosure.

Public Disclosure: The publication of vulnerability details after fixes have been implemented or after the agreed timelines have expired.

3. Reporting Process

3.1 How to Report a Vulnerability

- Send a detailed report to: security@livingpackets.com
- For enhanced confidentiality, encrypt your report with our public PGP key (available upon request)

3.2 Ideal Report Content

- Detailed description of the vulnerability and its impact
- Steps to reproduce the issue (HTTP requests, screenshots, or other details)
- Affected product version(s)
- Proof of concept or demonstration (if possible)
- Researcher's contact information

4. Timeline and Deadlines

Step	Timeline
Acknowledgment of receipt	Within 72 hours of receipt
Confirmation and assessment	Within 5 business days
Fix development	Variable depending on complexity
Coordinated disclosure deadline	90 days maximum after the update

5. Communication and Coordination

5.1 Points of Contact

- Email: security@livingpackets.com
- Security Officer: [Clement Mace, security@livingpackets.com]

5.2 Communication Language

We communicate in French and English. Please indicate your preference in your initial report.

We will maintain regular communication with the researcher throughout the process, with updates at least every two weeks.

5.3 Expected Conduct

- Do not access more data than necessary to demonstrate the vulnerability
- Do not modify or delete data
- Do not disrupt operations or services
- Respect the agreed coordinated disclosure timelines

6. Confidentiality and Privacy

- We will not disclose the researcher's identity without consent
- Information shared in vulnerability reports is treated confidentially
- The researcher's personal data is protected in accordance with applicable law (GDPR)
- Information will be disclosed internally only to those who need to know it

7. Public Disclosure Process

1. Timing: A public disclosure will only be made after the fix has been deployed, or 90 days after the initial notification, whichever occurs first
2. Coordination: We will coordinate with the researcher on the public disclosure text
3. Recognition: With authorization, we will credit the researcher in our security advisories
4. Exceptions: If we discover active exploitation, we may expedite disclosure

8. Exclusions and Limitations

We are not able to accept reports for:

- Client-side configuration issues (misconfiguration by the user)
- Issues affecting outdated or unsupported versions
- Physical or premises security issues
- Spam or denial-of-service attacks
- Issues arising from misuse or non-compliance with the terms of use

9. Legal Protection

We will not pursue legal action against security researchers who report vulnerabilities in good faith and in accordance with this policy. This includes temporary access to systems to demonstrate the vulnerability, provided the researcher does not access any data beyond what is necessary for the demonstration.

10. Continuous Improvement

We regularly review this policy and gather feedback from security researchers. If you have suggestions for improving this process, please address them to our security team.

Last updated: 09/07/2026

Security Officer

Full name: Clement Mace

Title: Data Protection Officer