Coordinated Vulnerability Disclosure Policy

Our Commitment

Pleora Technologies is committed to maintaining the security and integrity of our products and services. We value the contributions of security researchers, customers, and partners who help us identify potential vulnerabilities and work with us to address them responsibly.

This Coordinated Vulnerability Disclosure (CVD) policy describes how to report security vulnerabilities to Pleora and what you can expect from us in return.

Scope

This policy applies to security vulnerabilities affecting, including but not limited to:

- Pleora products and software
- Firmware and embedded components
- Supporting services or interfaces required for product operation

Issues **outside the scope** of this policy include:

- Availability testing that disrupts internal corporate infrastructure
- Social engineering or phishing directed at Pleora personnel
- Physical security of Pleora facilities or staff
- Vulnerabilities in third-party products not developed or maintained by Pleora

---

How to Report a Vulnerability

If you believe you have discovered a security vulnerability, please report it to us by emailing our Compliance Team: compliance@pleora.com.

Include as much information as possible, such as:

- Product name and version
- Detailed description of the vulnerability
- Steps to reproduce (if available)
- Potential impact
- Any evidence of exploitation
- Your preferred contact information

Please submit reports in English where possible.

Responsible Disclosure Expectations

We ask that reporters:

- Act in good faith and avoid privacy violations, data destruction, or service disruption
- Refrain from publicly disclosing the vulnerability until Pleora has had a reasonable opportunity to investigate and remediate the issue
- Provide sufficient detail to allow us to reproduce and assess the vulnerability

---

Our Response Process

When a potential security vulnerability is reported to Pleora, we will make reasonable efforts to:

1. **Log and review** the report through our security and compliance processes
2. **Assess and triage** the reported issue to determine validity, impact, and severity
3. **Escalate internally** through defined alerting and response workflows where appropriate
4. **Coordinate reporting** with relevant authorities where required under applicable legal or regulatory obligations
5. **Develop mitigations or corrective actions** for confirmed vulnerabilities
6. **Communicate guidance to affected customers** when appropriate
7. **Support coordinated disclosure practices** that prioritize user protection and responsible remediation

We may contact you for clarification or additional technical details during our investigation.

Coordinated Disclosure

Where appropriate, Pleora supports coordinated disclosure timelines that balance transparency with user protection. Disclosure timing may depend on factors such as:

- Severity and exploitability
- Availability of mitigations or patches
- Regulatory or customer-impact considerations

Pleora retains discretion to determine appropriate disclosure timing in line with user protection and regulatory obligations.

Pleora Technologies Inc.
450 March Road., Suite 500
Kanata, Ontario K2K 3K2

+1.613.270.0625
info@pleora.com
pleora.com

Safe Harbor

Pleora will not pursue legal action against individuals who:

- Engage in good-faith security research
- Follow this disclosure policy
- Do not exploit vulnerabilities beyond what is necessary for validation
- Do not violate applicable laws or regulations

This policy is intended to provide assurance that responsible security research is welcome and encouraged.

Changes to This Policy

Pleora may update this policy from time to time. The most current version will always be published on our website.

Thank You

We appreciate the efforts of the security community in helping keep Pleora products secure and our customers protected.

Pleora Technologies Inc.
450 March Road., Suite 500
Kanata, Ontario K2K 3K2

+1.613.270.0625
info@pleora.com
pleora.com