Coordinated Vulnerability Disclosure Policy

This Coordinated Vulnerability Disclosure (CVD) policy outlines Opticon's commitment to product security and our strict alignment with the Regulation (EU) 2024/2847 also known as EU Cyber Resilience Act (CRA).

We highly appreciate the contribution of external security researchers, ethical hackers and downstream users who help to make our digital ecosystem more secure.

This policy is intended to provide clear information about discovering and reporting vulnerabilities in Opticon products with digital elements in a structured, safe and lawful manner.

---

1. Purpose and commitments

Opticon designs, manufactures, distributes and services high-performance barcode scanning equipment, enterprise mobile computers and electronic shelf label solutions. In strict accordance with EU CRA Annex I, Part II(5) and Article 14 obligations, Opticon implemented a documented Coordinated Vulnerability Disclosure (CVD) process to manage security risks throughout Opticon products' defined lifecycles.

We pledge to:

- **Human-monitored contact:**
  - Provide a reliable, human-monitored single point of contact for security reporting.
- **Prompt remediation:**
  - Address validated vulnerabilities without undue delay through security updates, software patches or temporary risk-mitigation workarounds.
- **Safe harbor protections:**
  - Protect reporting parties who adhere to this policy under clear safe harbor rules.
- **Regulatory compliance:**
  - Opticon will comply with the CRA reporting obligations for actively exploited vulnerabilities and severe incidents, including the applicable 24-hour early-warning, 72-hour notification and final-report deadlines, through the European Union Agency for Cybersecurity (ENISA) CRA Single Reporting Platform (SRP) or any legally applicable reporting mechanism.

---

2. Scope

This policy applies to all relevant hardware products, embedded firmware and standalone software applications designed, manufactured or commercially distributed by Opticon within the European Union single market.

Summary of products in scope:

- **Scan engines:**
  - Such as MDI-series, MDL-series and MDC-series, Q-250.

- **Fixed mount:**
  - Such as NLB-series, RLB-series, NLV-series.
- **Presentation scanners:**
  - Such as M-series, P-series.
- **Companion scanners:**
  - Such as OPN-series.
- **Handheld scanners:**
  - Such as L-series, C-series, OPR-series wired and wireless variants.
- **Handheld terminals:**
  - Such as OPH-series.
- **Enterprise mobile computers:**
  - Such as H-series.
- **Electronics shelf label solutions:**
  - Such as EBS-series, EE-series, SE-series.
- **Standalone software:**
  - Such as ESL server, Opticonnect, Appload, SDK's and similar software.

---

3. Rules of engagement and safe harbor

To minimize risks to Opticon customers, business partners and internal systems, all security testing must respect the following boundaries:

- **No disruption:**
  - Do not perform Denial of Service (DoS/DDoS) attacks, brute-force testing, or use automated tools that degrade device infrastructure performance.
- **Data privacy:**
  - Stop testing immediately if you accidentally access confidential data, personally identifiable information or trade secrets. Do not view, alter, copy, or store customer data.
- **No social engineering:**
  - Physical security testing (e.g., office tailgating), social engineering, or phishing against Opticon employees, suppliers, or customers is strictly forbidden.
- **CRA safe harbor commitment:**
  - If you conduct your security research in good faith, avoid harming downstream users, and comply fully with this policy before making information public, Opticon will treat your research as authorized. We will not initiate legal action regarding your research under applicable anti-hacking laws.

4. How to report a vulnerability

To comply with the CRA requirement for open, non-automated communication, reporters can reach our security response team directly by email.

- **Email:**
  - Email your findings directly to **psirt@opticon.com**.

Required Submission Details

To accelerate evaluation and remediation, your submission must provide clear technical context:

- **Product Identification:**
  - Such as product model name, serial number, software version.
- **Vulnerability Mechanics:**
  - The underlying technical class of the flaw (e.g., buffer overflow, improper input validation).
- **Proof of Concept:**
  - A clear and detailed step-by-step description, log files, or functional script to safely replicate the issue.
- **Active Exploitation:**
  - Explicitly state if you have observed or possess reliable evidence that this flaw is currently actively being exploited in the field.

5. Process and timelines

Opticon handles all reported vulnerabilities through a structured, time-sensitive triage process aligned with industry benchmarks to ensure realistic enforcement.

- **Acknowledgement:**
  - You will receive a human response confirming receipt of your submission within **5 business days**.
- **Triage status update:**
  - Within **10 business days**, our Product Security Incident Response Team (PSIRT) will provide detailed feedback on the outcome of the initial assessment.
- **Early Warning:**
  - If we become aware of an active exploitation, Opticon will submit an early warning to Enisa via SRP within 24 hours.
- **Vulnarability notification:**
  - We provide more details about the vulnerability to Enisa via SRP within 72 hours.

- **Remediation target:**
  - Opticon aims to design, test, and commercially deploy signed security patches or alternative risk-mitigation measures within a reasonable timeframe from the initial triage and may depend on the technical complexity. If feasible, we will verify the effectiveness of the remediation with the reporter.

- **Final reporting:**
  - Once the remediation is available, we will submit the final report to ENISA via the SRP within 14 days.

---

6. Coordinated public disclosure and advisories

In compliance with EU CRA Annex I, Part II(4), Opticon prioritizes the systemic distribution of information regarding resolved vulnerabilities to limit downstream consumer exposure.

- **Coordinated disclosure embargo:**
  - Reporters must agree to keep details of verified vulnerabilities strictly confidential until Opticon formally releases a patch or alternative mitigation strategy to affected users.

- **Public advisories:**
  - Once fixed, Opticon will publish a clear security advisory containing the Common Vulnerabilities and Exposures (CVE) identifier, vulnerability severity score (CVSSv3.1/v4.0), and remediation or workaround steps.

- **VEX (Vulnerability Exploitability eXchange):**
  - Whenever possible, Opticon issues advisories using machine-readable VEX formats. In alignment with regulatory compliance, these advisories map directly to internal Software Bill of Materials (SBOM) records maintained for market surveillance authorities.

- **Researcher recognition:**
  - On request, Opticon will publicize credit to the discovering party in our official Security Advisory notes, provided the researcher adhered fully to this policy during disclosure.

---

7. Document control and governance

This policy is owned and maintained by Opticon and will be updated regularly to reflect changes in regulatory standards, products or European Commission guidance documentation.

- **CVD version:** 1.00
- **Effective date:** 1 September 2026
- **Next review:** 1 March 2027
