Vulnerability Disclosure Policy

pursuant to the Regulation (UE) 2024/2847 – Cyber Resilience Act

Company	**APPLIED**
Applicability	Applied Group
Document Domain	ISMS COMPL
Document Code	APPL-COMPL-PL-003
Full Document Title	APPL-COMPL-PL-003-Vulnerability Disclosure Policy-v01
Document Title	Vulnerability Disclosure Policy
Version	1 - 14/07/2026
Language	English
Approved by	Executive Committee
Author	Cyber Security & Compliance Manager
Approval Date	14/07/2026
Data Classification	Public

DOCUMENT REVISION HISTORY

Version	Date	Author	Note
0.1	14/07/2026	Cyber Security & Compliance Manager	Document creation
0.1	14/07/2026	Executive Committee	Document approval

1. Purpose

Applied recognizes the importance of collaborating with customers, partners, security researchers, and other qualified parties to continuously improve the security of its products with digital elements.

This Vulnerability Disclosure Policy (VDP) defines the process for reporting potential security vulnerabilities to Applied and describes the principles governing their assessment, management, and remediation.

The objectives of this Policy are to:

- facilitate the timely identification of vulnerabilities;
- promote coordinated and responsible vulnerability disclosure (Coordinated Vulnerability Disclosure – CVD);
- support a structured vulnerability reporting and handling process;
- reduce the risks arising from the potential exploitation of vulnerabilities; and
- contribute to compliance with applicable requirements, including Regulation (EU) 2024/2847 (Cyber Resilience Act).

2. Scope

This Policy applies to vulnerability reports concerning products with digital elements developed and marketed by Applied S.r.l.

Where Applied receives vulnerability reports relating to products with digital elements developed by third-party manufacturers and distributed by the Company, such reports will be handled in accordance with the roles and responsibilities established under Regulation (EU) 2024/2847 and, where appropriate, shared with the relevant manufacturer.

This Policy does not constitute authorization to conduct penetration testing, automated vulnerability scanning, or any other intrusive activities against the systems, products, or infrastructure of Applied S.r.l.

3. Principles of Responsible Vulnerability Disclosure

Applied promotes a Responsible Vulnerability Disclosure approach by encouraging the timely and responsible reporting of identified security vulnerabilities.

Individuals submitting a vulnerability report are expected to act in good faith and to:

- provide accurate and sufficient information to enable the analysis and validation of the reported vulnerability;
- limit any verification activities to the minimum necessary to demonstrate the existence of the vulnerability;
- refrain from any actions that could compromise the availability, integrity, or confidentiality of systems or data;
- avoid intentionally accessing personal data or confidential information; and
- keep technical information relating to the reported vulnerability confidential until Applied has completed its vulnerability handling activities or unless otherwise agreed between the parties.

4. Vulnerability Reporting Process

Security vulnerabilities should be reported through the following dedicated channel: **cybersecurity@applied.it**

To enable an effective assessment, vulnerability reports should include, where available:

- a description of the vulnerability;
- the affected product;
- the version of the affected product or component;
- a description of the potential impact;
- the steps required to reproduce the issue;
- logs, screenshots, or other supporting technical documentation; and
- the reporter's contact details.

Incomplete reports may require additional information before they can be assessed.

5. Vulnerability Management Process

Applied manages reported vulnerabilities through a documented Vulnerability Management process.

Each vulnerability report is:

- logged and acknowledged;
- subject to technical verification;

- assessed to determine its validity, potential impact, and level of risk;
- classified according to appropriate severity criteria;
- addressed through corrective actions or mitigation measures; and
- monitored until the vulnerability management process has been completed.

All activities performed and decisions made are documented in accordance with the applicable internal procedures.

Where a reported vulnerability is found to be already known, already remediated, or a duplicate of a previously submitted report, Applied may close the report and notify the reporter accordingly.

6. Vulnerability Assessment and Remediation

La valutazione della vulnerabilità tiene conto, tra gli altri elementi, di:

- probabilità di sfruttamento;
- impatto sulla sicurezza del prodotto;
- disponibilità di misure di mitigazione;
- presenza di condizioni che aumentino il rischio;
- dipendenze da componenti o fornitori terzi.

In funzione della valutazione effettuata, Applied potrà adottare una o più delle seguenti misure:

- correzioni software;
- aggiornamenti di sicurezza;
- misure di mitigazione temporanee;
- comunicazioni agli utilizzatori;
- altre misure tecniche o organizzative ritenute appropriate.

The assessment of a reported vulnerability takes into account, among other factors:

- the likelihood of exploitation;
- the impact on the security of the affected product;
- the availability of mitigation measures;
- the existence of conditions that may increase the associated risk; and
- dependencies on third-party components or suppliers.

Based on the outcome of the assessment, Applied may implement one or more of the following measures:

- software fixes;
- security updates;

- temporary mitigation measures;
- communications to users; and
- any other technical or organizational measures deemed appropriate.

7. Coordinated Vulnerability Disclosure

Applied supports a Coordinated Vulnerability Disclosure (CVD) process.

To protect users of its products and reduce the risk of vulnerability exploitation, reporters are requested not to publicly disclose technical information relating to a reported vulnerability until Applied has had a reasonable opportunity to:

- verify the reported vulnerability;
- assess the associated risk;
- implement any necessary corrective actions or mitigation measures; and
- inform affected users, where appropriate.

Where feasible, Applied will work with the reporter to agree on the timing and manner of any public disclosure of the vulnerability.

8. Response Timelines

Except in exceptional circumstances, Applied undertakes to:

- acknowledge receipt of a vulnerability report within five (5) business days;
- complete an initial assessment within ten (10) business days; and
- keep the reporter informed of the status of the vulnerability handling process whenever there are significant developments.

The time required to analyze and remediate a reported vulnerability may vary depending on its technical complexity, severity, and any involvement of third parties.

9. Reports concerning Third-Party Products

Where a vulnerability report concerns products with digital elements developed by third parties and distributed by Applied, the Company will assess and handle the report in accordance with its role within the supply chain.

Where appropriate, Applied will cooperate with the relevant manufacturer by sharing only the information strictly necessary for the management and remediation of the reported vulnerability, in compliance with applicable legal requirements and any contractual obligations.

10. Prohibited activities

This Policy does not authorize any activities that may compromise the security, availability, or proper functioning of Applied's products, systems, or infrastructure.

Reporters are expected to limit their activities to what is strictly necessary to identify and document the reported vulnerability and to refrain from any conduct that could cause harm to systems, data, or users.

11. Confidentiality and Protection of Personal Data

Applied S.r.l. processes the information received through vulnerability reports in accordance with the principles of confidentiality and uses such information solely for the purposes of assessing, managing, and remediating the reported vulnerabilities.

Any personal data provided as part of a vulnerability report will be processed in accordance with Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) and other applicable data protection laws.

12. Contacts

Security vulnerability reports should be submitted to Applied's Cybersecurity Team using the following dedicated email address: **cybersecurity@applied.it**

13. Policy Review and Updates

This Policy is reviewed periodically and updated, where necessary, to ensure its continued alignment with applicable legal requirements, technological developments, and the internal processes of Applied S.r.l.

The current version of this Policy is made available through the Company's official communication channels