EMMECI

a coesia company

Coordinated Vulnerability Disclosure Policy

EMMECI
a coesia company

Coordinated Vulnerability Disclosure Policy

Index

1. Purpose 3
2. Applicability 3
   2.1 Revision and Date of Application
3. Reference Documents 3
4. Definitions 3
5. General Principles 4
6. Vulnerability Reporting 5
   6.1 How to Report a Vulnerability
   6.2 Contents of the Vulnerability Report
7. Vulnerability analysis and remediation 5
   7.1 Product security software updates
8. Disclosuring information on vulnerabilities 6
9. Permitted and forbidden behavior 7
   9.1 Permitted behavior
   9.2 Forbidden behavior
10. Acknowledgment of a person reporting a vulnerability 8
11. Updates to the Coordinated Vulnerability Disclosure Policy 8

Date of release: 11/09/2026

1. Purpose

Purpose of this Coordinated Vulnerability Disclosure Policy is to describe how EMMECI S.p.A. receives, manages and discloses the vulnerabilities of products with digital elements manufactured by EMMECI S.p.A.

2. Applicability

The provisions outlined in this Coordinated Vulnerability Disclosure Policy apply to products with digital elements manufactured by EMMECI S.p.A. and falling within the scope of Regulation (EU) 2024/2847.

2.1 Revision and Date of Application

This Coordinated Vulnerability Disclosure Policy is Revision 0 and shall enter into force on 11 September, 2026.

3. Reference Documents

- Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024, concerning horizontal cybersecurity requirements for products with digital elements, amending Regulations (EU) 168/2013 and (EU) 2019/1020, and Directive (EU) 2020/1828 (Cyber Resilience Regulation).
- UNI CEI EN ISO/IEC 29147 :2020 : Information technologies. Security techniques. Vulnerability disclosure.

4. Definitions

- *Product with digital elements:* Any software or hardware product and related remote data processing solutions, including software or hardware

components, placed on the market separately. For the sake of brevity, the term "product" will be used hereinafter.

- *Vulnerability:* A weakness, susceptibility, or defect in ICT products[1] or services that can be exploited by a cyber threat.
- *Exploitable vulnerability:* Vulnerability that can be used effectively by an attacker under practical operating conditions.
- *Actively exploited vulnerability:* Vulnerability with reliable evidence that an attacker exploited it in a system, without the system owner's authorization.
- *Incident:* Event that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, computer and network systems[2].
- *Severe incident:* An incident having an impact on the security of the product with digital elements shall be considered severe where[3]:
  - It negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or
  - It has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements.

5. General Principles

EMMECI S.p.A. recognizes the value of working together with the Cybersecurity research community and with the users of products manufactured by EMMECI S.p.A. and undertakes to:

- Promote responsible vulnerability reporting.
- Guarantee the confidentiality of the information received.
- Handle reports with diligence, timeliness and impartiality.
- Coordinate public disclosure of vulnerabilities, where appropriate.
- Refrain from taking legal action against anyone reporting vulnerability, acting in compliance with this Coordinated Vulnerability Disclosure Policy and the applicable laws.

[1] ICT: Information and Communication Technology.

[2] Directive (EU) 2022/2555, Article 6(6).

[3] Regulation (EU) 2024/2847, Article 14.

6. Vulnerability Reporting

6.1 How to Report a Vulnerability

EMMECI S.p.A. has established a procedure by which each customer can report a vulnerability that has emerged on the products it supplies:

The procedure provides that the customer can write an email to the assistenza.clienti@emmeci.it address reporting a new vulnerability encountered on his machine according to the procedures in point 6.2.

Receipt of the report will be confirmed to the person who reported the vulnerability via an email from the assistenza.clienti@emmeci.it address within seven days.

6.2 Contents of the Vulnerability Report

The vulnerability report must contain at least the following information:

- E-mail address where the person reporting the vulnerability can be reached
- ID of the product on which the vulnerability was found, and the product version, if relevant
- Description of the vulnerability detected and the conditions in which it occurs
- Any other information useful to contextualize the conditions in which the vulnerability occurs

7. Vulnerability analysis and remediation

Vulnerabilities that have been reported to the contact points indicated in Section 6.1 are promptly analyzed by EMMECI S.p.A. The analysis may show that:

- The vulnerability concerns a component integrated into the product; in this case, EMMECI S.p.A. acknowledges the person who reported the vulnerability by specifying that the vulnerability has been reported to the

manufacturer of the affected component and indicating any other action taken to mitigate the impact of the vulnerability;

- No software updates or product modifications are required; in this case, EMMECI S.p.A. acknowledges the person who reported the vulnerability by explaining why it cannot compromise the IT security of the product;
- The vulnerability concerns a product for which the support period has ended; in this case, EMMECI S.p.A. acknowledges the person who reported the vulnerability by explaining that the support period of the product has ended;
- The vulnerability concerns an obsolete product for which it is not possible to apply software updates or make hardware changes; in this case, EMMECI S.p.A. assesses what measures can be taken to minimize the security risks of the IT and, if necessary, notifies the known users of the product.

The vulnerability investigation and remediation process should normally be completed within 30 days; if this process takes longer, the person reporting the vulnerability will receive an email from the assistenza.clienti@emmeci.it address every 15 days with appropriate updates on the status of the vulnerability analysis and remediation process.

7.1 Product security software updates

Based on the analyses carried out according to the methods described in Section 7, EMMECI S.p.A.:

- Prepares the necessary security software updates
- Identifies the products to which the updates will apply
- Identify the product users
- Installs the software updates through remote support, if necessary

8. Disclosuring information on vulnerabilities

Once a security software update is available to resolve the reported vulnerability, EMMECI S.p.A. will provide:

- Send an email to the entity that reported the vulnerability to communicate the conclusion of the modification process and the release of the resolution SW update

- Define together with the person who reported the vulnerability the timing and methods for adopting the update.
- Identify whenever possible all individuals using this product with the specific SW version that is subject to the reported vulnerability.
- If the vulnerability identified poses a risk to the security of individuals, use e-mail messages to ensure that purchasers and known users of the affected products are made aware of the vulnerabilities identified on the specific product and describe its severity and specific risks.
- Provide guidance on how to fix vulnerabilities (e.g., installing software updates, configuring the product, etc.).

9. Permitted and forbidden behavior

9.1 Permitted behavior

Security testing on the system being analyses is allowed only to the extent strictly necessary to prove the existence of a vulnerability, without negatively affecting the systems, data and users.

9.2 Forbidden behavior

It is forbidden to:

- Access, modify or extract personal, confidential or sensitive data from the system not necessary to report a vulnerability.
- Compromise service availability on the system being analyzed (e.g., through denial-of-service attacks).
- Introduce malware into the system being analyzed.
- Copy, modify or delete data in the system being analyzed.
- Make changes to the system being analyzed.
- Repeatedly access the system being analyzed or share the login credentials to the system being analyzed with other people.
- Execute brute force attacks to gain access to a system.
- Exploit the vulnerability for purposes other than reporting.
- Publicly disclose the vulnerability without EMMECI S.p.A.'s prior written authorization.

10. Acknowledgment of a person reporting a vulnerability

Without prejudice to the fact that all information received shall be processed exclusively for the purpose of managing vulnerabilities, in compliance with Regulation (EU) 2016/679 (GDPR), EMMECI S.p.A.'s sole discretion, a person reporting a vulnerability, and providing valid and compliant contributions to this Coordinated Vulnerability Disclosure Policy, may be acknowledged by:

- Being mentioned in public thank you lists, with the person's explicit authorization.
- Being mentioned in the vulnerability disclosure documents (see Section 8), with the person's explicit authorization.
- Possible access to incentive programs, where applicable.

11. Updates to the Coordinated Vulnerability Disclosure Policy

This Coordinated Vulnerability Disclosure Policy may be amended or updated at any time.
The current version is published on the Company's website, and shall be binding starting on the date of application indicated in the Coordinated Vulnerability Disclosure Policy.