Vulnerability Disclosure Policy

Aligned with Regulation (UE) 2024/2847 Cyber Resilience Act (CRA)

1 Summary

2 Purpose

This Vulnerability Disclosure Policy ("Policy" or "VDP") defines the manner in which **OCME Srl** (hereinafter referred to as the "Company") receives, evaluates, manages, and communicates reports of cybersecurity vulnerabilities relating to its products with digital elements, including, in particular, machinery, automation systems, and associated software and firmware components.

This Policy has been established in accordance with Regulation (EU) 2024/2847 of the European Parliament and of the Council (Cyber Resilience Act, "CRA"), which requires manufacturers of products with digital elements to implement a vulnerability management process throughout the entire product lifecycle, including a coordinated vulnerability disclosure channel (Article 13) and obligations for timely notification to ENISA and the designated CSIRT in the event of actively exploited vulnerabilities or severe incidents (Article 14).

The Company undertakes not to initiate legal proceedings against any individual or entity that, acting in good faith and in compliance with this Policy, reports a potential vulnerability identified in the Company's products.

3 Scope of Application

The Policy applies to all products with digital elements placed on the market by the Company, including machines and automation systems equipped with electronic components, network connectivity, or remote communication interfaces. The following sections clarify which products and systems fall within the scope of this Policy and which are excluded from it.

3.1 Products Covered by this Policy

This Policy applies to all products manufactured by the Company and offered to its customers, including:

- Entire automated machines, including, in particular Filling machines (models: Libra), secondary packaging and handling systems (models: Vega; Altair; Cygnus; Chamaeleon; Scorpius), palletizing and depalletizing systems (models: Pegasus; Perseus; Orion; Ares; Mizar; Dorado), decrating and crating systems (models: Leo), conventional conveying systems (primary packaging product conveyors, secondary packaging product conveyors, and pallet conveyors) and automated logistics handling systems using autonomous vehicles (models: Auriga);
- supervisory and monitoring software products, including Pallet labeling solutions, Remote line start-up system (Job Executor), Plant supervision systems.

Excluded from the scope of this Policy are all systems that are neither manufactured by the Company nor integrated into the solutions supplied by the Company. By way of example, but not limited to, are excluded customer information systems that are unrelated to the Company's products, such as ERP and MES systems,

and more generally, all Information Technology (IT) systems and any third-party products, systems, or services that fall outside the Company's scope of supply.

3.1.1 Authorization for Voluntary Vulnerability Testing

The execution of cybersecurity verification, analysis, assessment, or testing activities on the Company's products falling within the scope of this Policy is not permitted unless expressly authorized in advance by the Company through a written agreement setting out the scope, limitations, and conditions of the authorized activities.

The Company reserves the right to require the presence of an authorized Company representative, either on-site or remotely, throughout the entire duration of the testing activities.

4 Key Definitions

- Product with Digital Elements: A software or hardware product, including the associated remote data processing solutions, as well as software or hardware components placed separately on the market, as defined in Article 3(1) of the Cyber Resilience Act (CRA).
- Manufacturer: Any natural or legal person who develops or manufactures products with digital elements, or has them designed, developed, or manufactured, and markets them under its own name or trademark, whether for payment, free of charge, or through any other form of monetization, as defined in Article 3(13) of the CRA. For the purposes of this Policy, the Company acts as the manufacturer of the products described in Section 3.1.
- Vulnerability: A weakness, susceptibility, or defect in a product with digital elements that may be exploited by a cyber threat.
- Actively Exploited Vulnerability: A vulnerability for which credible evidence exists that a malicious actor is actively exploiting it in a product without the consent of the system owner.
- Severe Incident: An event having an actual adverse impact on the security of a product with digital elements, according to the criteria established by the European Commission and ENISA pursuant to Article 14 of the CRA.
- Coordinated Vulnerability Disclosure (CVD): A structured process through which vulnerabilities are reported to the manufacturer, allowing sufficient time for diagnosis and remediation before the public disclosure of the vulnerability details.
- PSIRT (Product Security Incident Response Team): The Company's internal team responsible for receiving, assessing, and managing vulnerability reports and product security incidents.

- Designated CSIRT: The national Computer Security Incident Response Team designated under the CRA as the coordinating authority for the receipt of notifications, in cooperation with ENISA.

5 How to Report a Vulnerability or Incident

Reports may be submitted through the following dedicated channel established by the PSIRT:

- E-mail: cra.compliance@ocme.com

Despite the dedicated contact channel indicated above, customers may continue to use the communication channels customarily employed in their interactions with the Company. In accordance with the Company's internal reporting management procedures, any communication, report, or request received through channels other than the dedicated one will nevertheless be accepted and handled in accordance with the same processes applicable to reports submitted through the official channel, ensuring the application of the same management, assessment, and response procedures.

However, to ensure the proper and effective handling of vulnerability reports, reporters are strongly encouraged to use the official channel indicated above. For reports received through alternative channels, the timelines established by this Policy, and the related operational activities, shall commence from the date on which the report is formally registered and made available to the PSIRT through the Company's internal escalation process. The Company does not guarantee compliance with the timelines established by this Policy during the period between the receipt of a report through a non-dedicated channel and its formal registration and acceptance by the PSIRT.

To enable proper assessment and management of a report, the reporter is requested to provide, at a minimum, the following information:

1. Customer name, production facility, and production line where the machine or software concerned by the report is installed or used
2. Product name, model, and serial number of the machine or software concerned by the report, as indicated on the applied CE nameplate. For example:
   OCME Altair HT, serial number 1100045A01
3. Type of notification, specifying whether the report concerns an actively exploited vulnerability or a severe cybersecurity incident
4. Technical description of the reported vulnerability or incident, including, where available, the relevant classification (for example, CWE).
5. Information and steps necessary to reproduce the vulnerability or to understand the reported event, if known at the time of reporting.
6. Logs, technical evidence, screenshots, or any other relevant supporting documentation available
7. Assessment of the potential or observed impact on the confidentiality, integrity, and availability of data and systems.
8. Any indicators of active exploitation that have already been observed

9. Contact details of the reporter, preferably an email address, to enable requests for clarification and subsequent communications relating to the management of the report

Should a report be incomplete, inaccurate, or fail to contain the minimum information required for technical assessment, the Company may request additional information or clarification from the reporter. The absence of essential information may result in delays in the analysis, classification, and management of the report.

5.1 Reporter Personal Data Processing

Any personal data provided by the reporter as part of a report (for example, name and contact details) shall be processed by the Company, acting as the data controller, solely for the purposes of managing, assessing, and responding to the report, in accordance with Regulation (EU) 2016/679 (GDPR) and the applicable national data protection legislation. For further information regarding the processing of personal data, the rights of the data subject, and data retention periods, please refer to the Company's Privacy Notice.

6 Internal Management Process (PSIRT)

The PSIRT manages each report through a structured process consisting of the following phases:

1. Receipt and registration of the report within the Company's internal tracking system.
2. Initial triage, including verification of the report's validity, relevance to this Policy, and identification of the affected products and versions.
3. Communication with the reporter regarding the outcome of the initial assessment and, where necessary, a request for additional information.
4. Determination of whether the vulnerability is actively exploited or qualifies as a severe incident pursuant to Article 14 of the CRA, with the consequent activation of the ENISA/CSIRT notification workflow described in Section 6.1.
5. Identification of the appropriate corrective measure, including a security patch, firmware update, or compensating mitigation measure.
6. Communication to affected customers and users, where appropriate, including through the publication of a Security Advisory on the Company's website, providing guidance on the actions to be taken.
7. Closure of the report and, where agreed, coordinated public disclosure of the vulnerability.
8. Post-incident analysis (lessons learned) and update of internal processes, where necessary, to improve the effectiveness of vulnerability and incident management activities.

6.1 Reporting Obligations and Timelines for ENISA Notifications (Article 14 CRA)

Where a vulnerability managed by the PSIRT is determined to be actively exploited, or where a severe cybersecurity incident affecting a product with digital elements occurs, the Company, acting as the manufacturer, shall notify ENISA through the single reporting platform established pursuant to Article 16 of the CRA, in accordance with the following timelines:

Deadline	Requirement	Minimum Content
Within 24 hours	Early warning notification	Preliminary notification to ENISA and/or the designated CSIRT through the Single Reporting Platform. The notification shall include the nature of the active exploitation or severe incident, the affected product(s), and the Member States potentially concerned. At this stage, the information may still be partially incomplete.
Within 72 hours	Follow-up Notification (Vulnerability/Incident Notification)	Update of the initial notification with any available information regarding severity, impact, indicators of compromise, and, where known, the corrective or mitigation measures already implemented or that can be implemented in the short term.
Within 14 days after the corrective measure becomes available (vulnerability)	Finale report	Detailed description of the vulnerability (cause, severity, CVSS score), confirmation that remediation has been completed, and, where relevant, mitigation measures made available to users.
Within 1 month of the initial notification (severe incident)	Final Severe Incident Report	Description of the incident, root cause, corrective measures implemented, and impact on the installed machine base, where relevant.

The obligation to notify actively exploited vulnerabilities and severe incidents pursuant to Article 14 of the Cyber Resilience Act (CRA) applies from 11 September 2026.

The PSIRT maintains a dedicated operational procedure to ensure compliance with these notification deadlines from the date on which the obligation becomes applicable.

7 Coordinated Public Disclosure

Where it is not possible to promptly and individually notify all parties affected by the same actively exploited vulnerability, or those who may be exposed to similar severe cybersecurity incidents, mitigation measures may be communicated publicly through Security Advisories published on the Company's website at

https://www.ocme.com/en/security-advisories.php

In all cases, the public disclosure date shall be agreed with the reporter, considering the time required to develop, validate, and distribute the corrective measure, which, in the industries in which the Company operates, may require extended timeframes.

The Company nevertheless undertakes not to delay public disclosure beyond what is strictly necessary to adequately inform users and ensure the security of the installed base of machines and software.

8 “Safe Harbor” Commitment

The Company considers vulnerability reporting activities to be lawful under this Policy when they are conducted in good faith and provided that:

- Vulnerabilities identified in products marketed by the Company are promptly reported through the channels specified in Section 5
- Vulnerability details are not publicly disclosed before the coordinated disclosure date agreed upon with the Company's PSIRT.

Subject to compliance with the above conditions, the Company will not initiate civil or legal proceedings against the reporter in connection with the reported vulnerability.

Any extortionate, threatening, coercive, or otherwise improper conduct inconsistent with the principles of good faith and fair dealing is strictly prohibited. Reporters shall not request, solicit, or demand rewards, financial compensation, benefits, or any other form of consideration that has not been expressly agreed in writing with the Company prior to the performance of the research or reporting activities. Furthermore, reporters undertake not to submit the same report repeatedly, nor to use different email addresses or other methods intended to make a report appear as though it originates from multiple distinct individuals or entities.

9 Policy Review and Updates

This Policy shall be reviewed on an annual basis, or whenever significant changes occur in the applicable regulatory framework, including any implementing guidance issued by ENISA or the European Commission concerning the Cyber Resilience Act (CRA).

In addition, the Policy shall be reviewed whenever lessons learned from incidents managed by the PSIRT indicate the need for updates or improvements to the Company's vulnerability management and incident response processes.

10 Contacts

- PSIRT: cra.compliance@ocme.com
- Security Advisories Website: https://www.ocme.com/en/security-advisories

- Registered Office: OCME Srl, via del Popolo 20/A – 43122 Parma (Italy)