

Vulnerability Disclosure Policy (VDP)					
Responsible Vulnerability Disclosure Policy					
Document date	Doc. No	Revision	Effective from	Template no	Page
09.09.2026	VDP_CRA_AETNA_EN_rev0.docx	0	10.09.2026	1.1-EN	1/11

Vulnerability Disclosure Policy

Aligned with Regulation (UE) 2024/2847

Cyber Resilience Act (CRA)

Purpose	To define the company policy for reporting cybersecurity vulnerabilities and severe incidents affecting the Company’s products with digital elements, in compliance with the European CRA.
---------	--

Vulnerability Disclosure Policy (VDP)					
Responsible Vulnerability Disclosure Policy					
Document date	Doc. No	Revision	Effective from	Template no	Page
09.09.2026	VDP_CRA_AETNA_EN_rev0.docx	0	10.09.2026	1.1-EN	2/11

1 Revision history

Revision	Data	Reason	Description
-	09.09.2026	First issue	First issue

Vulnerability Disclosure Policy (VDP)					
Responsible Vulnerability Disclosure Policy					
Document date	Doc. No	Revision	Effective from	Template no	Page
09.09.2026	VDP_CRA_AETNA_EN_rev0.docx	0	10.09.2026	1.1-EN	3/11

2 Contents

1	Revision history	2
2	Contents	3
3	Abbreviations.....	4
4	Purpose.....	5
5	Scope	5
5.1	Products covered by the Policy.....	5
5.1.1	Authorization for voluntary vulnerability testing	6
6	Key definitions.....	6
7	How to report a vulnerability or incident.....	7
7.1	Processing of the reporter's personal data.....	8
8	Internal management process (PSIRT)	8
8.1	ENISA reporting obligations and timelines (Article 14 CRA)	8
9	Coordinated public disclosure	9
10	Safe Harbor commitment.....	10
11	Policy review and update	10
12	Contacts	11

Vulnerability Disclosure Policy (VDP)					
Responsible Vulnerability Disclosure Policy					
Document date	Doc. No	Revision	Effective from	Template no	Page
09.09.2026	VDP_CRA_AETNA_EN_rev0.docx	0	10.09.2026	1.1-EN	4/11

3 Abbreviations

Abbreviations	Full wording	Description

Tabella 1 - Abbreviations

Vulnerability Disclosure Policy (VDP)					
Responsible Vulnerability Disclosure Policy					
Document date	Doc. No	Revision	Effective from	Template no	Page
09.09.2026	VDP_CRA_AETNA_EN_rev0.docx	0	10.09.2026	1.1-EN	5/11

4 Purpose

This Vulnerability Disclosure Policy (the "Policy" or "VDP") defines how **AETNA GROUP SPA** (hereinafter the "Company") receives, assesses, manages and communicates reports of cybersecurity vulnerabilities relating to its products with digital elements, particularly machines, automation systems and related software/firmware components.

The Policy has been prepared 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 adopt a vulnerability management process throughout the entire product life cycle, including a coordinated vulnerability disclosure channel (Article 13) and timely reporting obligations 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 action against anyone who, in good faith and in compliance with this Policy, reports a potential vulnerability identified in the Company's products.

5 Scope

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 what is included in and excluded from the scope of the Policy.

5.1 Products covered by the Policy

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

- complete automatic machines, secondary packaging systems, palletizing and depalletizing systems, pallet wrapping machines, primary-packaging product conveying systems, secondary-packaging product conveying systems, and pallet conveying systems.
- software products for the supervision and control of machines and lines.

Excluded from this Policy are all systems that are not manufactured by the Company or are not integrated into the solutions offered by the Company. By way of example, but not limitation, excluded systems include the customer's corporate information systems that are unrelated to the Company's products, such as ERP and MES systems and, in general, all IT-level systems, as well as anything supplied by third parties that is outside the Company's scope of supply.

Vulnerability Disclosure Policy (VDP)					
Responsible Vulnerability Disclosure Policy					
Document date	Doc. No	Revision	Effective from	Template no	Page
09.09.2026	VDP_CRA_AETNA_EN_rev0.docx	0	10.09.2026	1.1-EN	6/11

5.1.1 Authorization for voluntary vulnerability testing

The performance of verification, analysis, assessment or cybersecurity testing activities on the Company's products falling within the scope of this Policy is not permitted unless prior express authorization has been issued by the Company through a written agreement governing the methods, limits and conditions of the authorized activities.

The Company reserves the right to require the presence, either in person or remotely, of an appointed Company representative for the entire duration of the verification activities.

6 Key definitions

- **Product with digital elements:** a software or hardware product and its remote data processing solutions, including software or hardware components placed on the market separately, pursuant to Article 3(1) of the CRA
- **Manufacturer:** a natural or legal person who develops or manufactures products with digital elements, or has them designed, developed or manufactured, and markets them under its name or trademark, whether for payment, free of charge or through another form of monetization, pursuant to Article 3(13) of the CRA. For the purposes of this Policy, the Company acts as manufacturer of the products referred to in Section 5.1.
- **Vulnerability:** a weakness, susceptibility or flaw in a product with digital elements that can be exploited by a cyber threat.
- **Actively exploited vulnerability:** a vulnerability for which there is reliable evidence that a malicious actor is exploiting it in a product without the consent of the system owner.
- **Severe incident:** an event having an actual negative impact on the security of a product with digital elements, according to the criteria defined by the European Commission/ENISA pursuant to Article 14 of the CRA.
- **Coordinated Vulnerability Disclosure (CVD):** a structured process through which vulnerabilities are reported to the manufacturer so that they can be diagnosed and remediated before public disclosure of the details.
- **PSIRT (Product Security Incident Response Team):** the internal Company team responsible for receiving, assessing and managing vulnerability reports and security incidents affecting products.
- **Designated CSIRT:** the national Computer Security Incident Response Team appointed as coordinator under the CRA for receiving notifications, in coordination with ENISA.

Vulnerability Disclosure Policy (VDP)					
Responsible Vulnerability Disclosure Policy					
Document date	Doc. No	Revision	Effective from	Template no	Page
09.09.2026	VDP_CRA_AETNA_EN_rev0.docx	0	10.09.2026	1.1-EN	7/11

7 How to report a vulnerability or incident

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

- CRA Compliance - Systems Robopac - cra.compliance.systems@robopac.com
- CRA Compliance - Packers Robopac - cra.compliance.packers@robopac.com
- CRA Compliance - Palletizers Robopac - cra.compliance.palletizers@robopac.com

Without prejudice to the contact channels indicated above, the other communication channels normally used by customers in their dealings with the Company remain valid and may also be used. In accordance with the internal report-management procedures, any communication, report or request received through channels other than the dedicated channel will nevertheless be handled according to the same processes applicable to reports received through the official channel, ensuring the application of the same management, assessment and response processes.

However, to ensure the correct and effective handling of vulnerability reports, reporters are invited to use the official channel indicated above. For reports received through other channels, the timelines set out in this Policy and the related operational activities begin on the date on which the report is formally registered and made available to the PSIRT through the Company's internal forwarding process. The Company does not guarantee compliance with the timelines set out in this Policy for the period between receipt of the report through a non-dedicated channel and its formal acceptance by the PSIRT.

To enable the report to be assessed and managed correctly, the reporter is invited to provide the following minimum information:

1. Customer name, production site and production line where the machine or software concerned by the report is installed or used
2. Product, model and serial number of the machine or software concerned by the report, as shown on the applied CE nameplate. For example:
ROBOPAC Palwrapp 2, serial number C526030031
3. Type of notification: 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, its classification (for example, CWE).
5. Information and steps required to reproduce the vulnerability or understand the reported event, if known at the time of reporting.
6. Logs, technical evidence, screenshots or other relevant available documentation
7. Assessment of the potential or observed impact in terms of confidentiality, integrity and availability of data and systems.
8. Any indicators of active exploitation already observed
9. Reporter's contact details, preferably an email address, to allow requests for clarification and subsequent communication concerning management of the report

Vulnerability Disclosure Policy (VDP)					
Responsible Vulnerability Disclosure Policy					
Document date	Doc. No	Revision	Effective from	Template no	Page
09.09.2026	VDP_CRA_AETNA_EN_rev0.docx	0	10.09.2026	1.1-EN	8/11

If the report is incomplete, inaccurate or does not contain the minimum information needed for its technical assessment, the Company may request additions or clarification from the reporter. Missing essential information may delay the analysis, classification and management of the report.

7.1 Processing of the reporter's personal data

Any personal data provided by the reporter as part of a report, such as name and contact details, are processed by the Company, as data controller, exclusively for the purposes of managing, assessing and responding to the report, in accordance with Regulation (EU) 2016/679 (GDPR) and applicable national data-protection legislation. For further information on processing methods, data-subject rights and retention periods, please refer to the Company's privacy notice.

8 Internal management process (PSIRT)

The PSIRT manages each report through a structured process comprising the following stages:

1. Receipt and registration of the report in the internal tracking system.
2. Initial triage: verification of validity, relevance to this Policy and identification of the products/versions involved.
3. Communication to the reporter of the outcome of the initial checks and any request for additional information.
4. Determination of whether the vulnerability is actively exploited or attributable to a severe incident pursuant to Article 14 of the CRA, with consequent activation of the ENISA/designated CSIRT notification workflow described in Section 8.1.
5. Identification of the corrective measure (patch, firmware update or compensating mitigation).
6. Communication to affected customers/users, possibly also through a security advisory published on the website, with instructions on the actions to be taken.
7. Closure of the report and, if agreed, coordinated public disclosure.
8. Post-incident analysis (lessons learned) and process updates where necessary.

8.1 ENISA reporting obligations and timelines (Article 14 CRA)

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

Vulnerability Disclosure Policy (VDP)					
Responsible Vulnerability Disclosure Policy					
Document date	Doc. No	Revision	Effective from	Template no	Page
09.09.2026	VDP_CRA_AETNA_EN_rev0.docx	0	10.09.2026	1.1-EN	9/11

Deadline	Requirement	Minimum content
Within 24 hours	Early warning notification	Preliminary notification to ENISA/designated CSIRT through the single point of contact. The nature of the active exploitation or severe incident, the product(s) involved and the Member States potentially affected are communicated. 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 available information on severity, impact, indicators of compromise and, if known, corrective or mitigating measures already adopted or capable of being adopted in the short term.
Within 14 days after the corrective measure becomes available (vulnerability)	Final report	Detailed description of the vulnerability (cause, severity, CVSS), confirmation that remediation has been completed and, where relevant, mitigation measures made available to users.
Within one month of the initial notification (severe incident)	Final report on severe incident	Description of the incident, root cause, corrective measures applied and impact on the installed machine fleet, where relevant.

The obligation to report actively exploited vulnerabilities and severe incidents pursuant to Article 14 of the CRA applies from 11 September 2026.

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

9 Coordinated public disclosure

Where it is not possible to promptly and individually alert all parties affected by the same actively exploited vulnerability, or parties that may experience similar severe security incidents, mitigation measures are communicated publicly through security advisories made available on the Company portal at:

<https://www.robopac.com/it/security-advisories>

Vulnerability Disclosure Policy (VDP)					
Responsible Vulnerability Disclosure Policy					
Document date	Doc. No	Revision	Effective from	Template no	Page
09.09.2026	VDP_CRA_AETNA_EN_rev0.docx	0	10.09.2026	1.1-EN	10/11

In all cases, the public disclosure date is agreed with the reporter, considering the time needed to develop and distribute the correction, which may require extended timelines in the sectors in which the Company operates. The Company nevertheless undertakes not to delay disclosure beyond what is strictly necessary to inform and secure the installed fleet of machines and software.

10 Safe Harbor commitment

Under this Policy, the Company considers reporting activity conducted in good faith to be lawful when:

- vulnerabilities identified in a product marketed by the Company are promptly communicated through the channels specified in Section 7
- the vulnerabilities are not publicly disclosed before the coordinated disclosure date agreed with the Company's PSIRT.

Subject to compliance with these conditions, the Company will not bring civil or criminal legal action against the reporter in connection with the reporting activity performed.

Extortion, intimidating or otherwise improper conduct contrary to the principles of fairness and good faith is prohibited. The reporter must not request, solicit or demand rewards, financial compensation, benefits or other forms of consideration that have not been expressly agreed in writing with the Company before the research or reporting activities are performed. Furthermore, the reporter undertakes not to submit the same report repeatedly or to use different email addresses or other methods intended to make the report appear to originate from different parties.

11 Policy review and update

This Policy is reviewed annually, following significant changes to the applicable regulatory framework (including any implementing guidance from ENISA and the European Commission concerning the CRA), and in all cases following lessons learned from incidents managed by the PSIRT.

Vulnerability Disclosure Policy (VDP)					
Responsible Vulnerability Disclosure Policy					
Document date	Doc. No	Revision	Effective from	Template no	Page
09.09.2026	VDP_CRA_AETNA_EN_rev0.docx	0	10.09.2026	1.1-EN	11/11

12 Contacts

- PSIRT:

CRA Compliance - Systems Robopac - cra.compliance.systems@robopac.com

CRA Compliance - Packers Robopac - cra.compliance.packers@robopac.com

CRA Compliance - Palletizers Robopac - cra.compliance.palletizers@robopac.com

- Security Advisories website: <https://www.robopac.com/it/security-advisories>
- Registered office: Via Statale Marecchia n. 59, 47826 - Verucchio (RN) - Fraz. Villa Verucchio (Italy)