Automation & Robotics, a company incorporated under Belgian law and registered with the Verviers Commercial and Companies Register under number 0423 637 107, whose registered office is located at 111 rue des Ormes, B-4800 Verviers, Belgium, represented by its Chief Executive Officer (CEO)

Hereinafter referred to as « Automation & Robotics »,

has adopted this Coordinated Vulnerability Disclosure Policy (CVDP).

1. Scope and applicability

As part of its approach to strengthening the security of its products, services and information systems, Automation & Robotics, implements this Coordinated Vulnerability Disclosure Policy (CVDP).

This policy is approved by the Chief Executive Officer (CEO). Its operational implementation is ensured by the Product Security Incident Response Team (PSIRT), responsible for coordinating the receipt, analysis, assessment, handling and follow-up of vulnerability reports affecting products and components falling within the scope defined by this policy.

This policy establishes a framework enabling security researchers, customers, partners and other stakeholders to responsibly report security vulnerabilities identified in Automation & Robotics, products covered by this policy.

It does not constitute a general authorization to conduct testing, security analyses or access systems, equipment, infrastructures or environments belonging to Automation & Robotics, its customers or third parties.

Security research activities carried out under this policy must have as their sole purpose the identification, verification and coordinated reporting of vulnerabilities that may affect the security of Automation & Robotics, products. These activities must be carried out:

- in good faith,
- in a proportionate and controlled manner,
- without disrupting the normal operation of the products or environments concerned,
- without accessing, modifying, deleting, exfiltrating or disclosing data to which the participant is not authorized to have access,
- without compromising the availability, integrity or confidentiality of the systems concerned.

a) In-Scope Products and Services

Security research activities covered by this policy may exclusively concern:

- products listed in the Automation & Robotics catalogue and benefiting from active support.

Tel: +32 (0)87 322 323
Email :
www.ar.be

Automation & Robotics S.A.
P. Industriel de Lambermont,
Rue des Ormes, 111 – 4800 Verviers - Belgium

TVA : BE0423637107
Verviers

The inclusion of a product in the Automation & Robotics catalogue does not, in itself, constitute authorization to access the machines, equipment, systems or infrastructures on which such product is installed or operated by a customer or third party.

Any intervention involving a customer or third-party environment must be carried out under an appropriate authorization, an existing contract or a mandate explicitly permitting the performance of the operations concerned.

b) Participants Requirements

External participants may conduct research activities exclusively on products and Cloud services that they own, operate or legitimately use, provided that they strictly comply with the security scope and testing procedures defined in this policy.

Subject to good-faith compliance with this policy and its conditions, Automation & Robotics will not initiate civil or criminal proceedings against the participant in respect of research activities expressly authorized by this policy. This provision does not apply to acts exceeding the scope or conditions of this policy, nor to fraudulent or intentionally harmful behaviour.

Automation & Robotics employees and contractors appointed by Automation & Robotics as part of a separate assignment may conduct research activities within the scope of their duties or assignments, in accordance with the applicable internal procedures and within the limits of the authorizations granted.

The provisions of this policy relating to the independent nature of external participants do not prejudge the legal qualification applicable to employees, contractors or other persons acting within the framework of a separate contractual assignment entrusted by Automation & Robotics.

c) Excluded Products and systems

The following are excluded from the scope of this policy:

- systems, applications, infrastructures or services operated by third parties and not falling under Automation & Robotics responsibility,
- any product, system, equipment or service that is not explicitly included within the scope defined by this policy,
- products that have reached their official End of Support (EOS) date, according to the conditions defined below:
    - Products that have officially reached their End of Support (EOS) date, as communicated by Automation & Robotics, are no longer covered by the maintenance, remediation or provision of security updates commitments provided for under this policy.
    - Automation & Robotics may nevertheless receive and analyze reports relating to such products in order to assess, in particular, whether the identified vulnerability:

Tel: +32 (0)87 322 323
Email :
www.ar.be
Automation & Robotics S.A.
P. Industriel de Lambermont,
Rue des Ormes, 111 – 4800 Verviers - Belgium
TVA : BE0423637107
Verviers

- also affects a product or version that is still actively supported,
- concerns a component or functionality used in other products,
- falls under a legal or regulatory notification obligation.

The receipt or analysis of a report relating to an EOS product does not reinstate support for the product concerned and does not create any obligation for Automation & Robotics to provide a fix.

Any research activity carried out outside the scope explicitly defined by this policy is considered out of scope and does not benefit from the provisions set out in this CVDP

2. Mutual Obligations of the parties

Participants acting under this Coordinated Vulnerability Disclosure Policy (CVDP) undertake to comply with the conditions defined in this document.

This policy does not grant any general right of access to Automation & Robotics's systems, equipment or environments, or those of its customers or third parties. Activities carried out under this policy are limited to actions strictly necessary for the identification, verification and coordinated reporting of vulnerabilities affecting products explicitly covered by the policy.

a) Proportionality

The participant undertakes, in all its actions, to strictly comply with the principle of proportionality, meaning that it shall not disrupt the availability of services provided by the system or product and shall not make use of the vulnerability beyond what is strictly necessary to demonstrate the security flaw. The participant's actions must remain proportionate: if the demonstration is established on a small scale, there is no need to extend it further.

The purpose of this policy is not to permit the intentional access to the contents of computer data, communication data or personal data, and such access may only occur incidentally in the course of vulnerability research.

b) Prohibited Activities

As part of the responsible disclosure of vulnerabilities concerning automated systems, OT systems, industrial equipment, integrated products and Cloud products, the participant acting within the framework authorized by the CVDP undertakes to strictly comply with the rules below. Unless prior written authorization has Automation & Robotics granted by Automation & Robotics, the participant shall in particular refrain from:

- Modifying the configuration, parameters, firmware, programs, settings, control logic or any other element likely to affect the operation of programmable logic controllers (PLCs), human-machine interfaces (HMIs), industrial PCs, controllers, sensors, actuators or any other industrial equipment.

Tel: +32 (0)87 322 323
Email :
www.ar.be
Automation & Robotics S.A.
P. Industriel de Lambermont,
Rue des Ormes, 111 – 4800 Verviers - Belgium
TVA : BE0423637107
Verviers

- Installing, injecting or executing any unauthorized code or software, including any malware or other tool likely to alter the normal operation of the systems.
- Carrying out attacks or tests likely to cause unavailability or degradation of system performance, including denial-of-service (DoS/DDoS) attacks, load tests, fuzzing operations or any other intrusive test likely to affect the availability, stability or security of equipment and products.
- Attempting to obtain credentials, passwords, certificates, cryptographic keys or any other secret.
- Installing or using any device or mechanism enabling the interception, monitoring, recording or capture of communications.
- Causing physical movements of equipment (robots, conveyors, valves, motors, variable-speed drives).
- Accessing or attempting to access personal, commercial, technical or production data beyond what is strictly necessary to demonstrate the existence of the vulnerability.
- Maintaining persistent access (backdoor, created account, scheduled task, tunnel) after the vulnerability has Automation & Robotics demonstrated.
- Publicly disclosing a vulnerability before the coordinated disclosure process has Automation & Roboticsn completed.
- Using, retaining, disclosing or exploiting data, information or content originating from automated, industrial or OT systems where the participant knows or cannot reasonably disregard that such information was obtained without authorization.

If the participant wishes to use the assistance of a third party to conduct its research, it shall first ensure that such third party has read this policy and agrees to comply with all its provisions. The participant remains responsible for compliance with these obligations by any person acting on its behalf.

c) Confidentiality

The participant undertakes to strictly refrain from sharing, disseminating or disclosing to third parties any information, documentation or data collected under this vulnerability disclosure policy without the prior, explicit and written consent of the Automation & Robotics concerned. In particular, it is prohibited to reveal or disclose to third parties:

- data originating from automated, industrial or OT systems,
- communication data or network traffic captures,
- personal data,
- commercial, industrial or confidential information,
- any technical, functional or security information relating to the equipment, software, architectures or infrastructures analyzed,
- any information likely to facilitate the exploitation of a vulnerability.

Where the identified vulnerability is likely to affect other Automation & Robotics entities in Belgium and/or Europe, the participant or the responsible Automation & Robotics may, where appropriate, inform the Centre for Cybersecurity Belgium (CCB) at the following address:

Tel: +32 (0)87 322 323
Email :
www.ar.be
Automation & Robotics S.A.
P. Industriel de Lambermont,
Rue des Ormes, 111 – 4800 Verviers - Belgium
TVA : BE0423637107
Verviers

vulnerabilityreport@cert.be or the competent national or European authority, in accordance with the applicable coordination mechanisms.

Any communication relating to the vulnerability must be carried out responsibly and in a coordinated manner, in compliance with this policy and without prior public disclosure, unless otherwise agreed in writing by the Automation & Robotics concerned or required by law.

d) Good-Faith Conduct

Automation & Robotics undertakes to implement this policy in good faith and not to take civil or criminal legal action against a participant who complies with its conditions.

The participant acting within the framework authorized by the CVDP must be free from fraudulent intent, malicious intent, any intention to use the vulnerability beyond what is strictly necessary to demonstrate it, or any intention to cause damage to the system or its data.

In case of doubt regarding any of the conditions of our policy, the participant must contact our point of contact in advance and obtain its written approval before taking action.

e) Processing of Personal Data

The purpose of this policy is not to intentionally process personal data, but the participant may, even incidentally, be required to process personal data as part of its vulnerability research.

The processing of personal data has a broad scope and includes, in particular, the retention, modification, extraction, consultation, use or communication of any information that may relate to an identified or identifiable natural person. The “identifiable” nature of the person does not depend solely on the intention of the person processing the data to identify them, but on the possibility of identifying the person, directly or indirectly, using such data.

Thus, the participant may process personal data to a limited extent. In the event of processing such data, the participant undertakes to comply with the legal obligations relating to the protection of personal data and the conditions of this policy, in particular:

- The participant undertakes to limit the processing of personal data to what is necessary in view of the purpose of vulnerability research.
- The participant shall ensure that persons authorized to process personal data undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality.
- The participant shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The participant declares that it understands the risks associated with the implementation of this policy and that it has the expertise and experience necessary to test Automation & Robotics systems, equipment and products safely and in compliance with applicable laws and regulations.
- The participant shall reasonably cooperate with Automation & Robotics, to the extent that the information in its possession is relevant to the analysis and handling of the reported vulnerability. Such cooperation is limited to the information necessary for analysis, remediation and, where applicable, management of the consequences of the vulnerability.

Tel: +32 (0)87 322 323
Email :
www.ar.be

Automation & Robotics S.A.
P. Industriel de Lambermont,
Rue des Ormes, 111 – 4800 Verviers - Belgium

TVA : BE0423637107
Verviers

It does not constitute an obligation for the participant to assist Automation & Robotics in fulfilling its obligations as a data controller within the meaning of the GDPR.

- Where, as part of its research, the participant discovers or suspects that a vulnerability has enabled unauthorized access to personal data, it shall inform Automation & Robotics as soon as possible at vulnerabilityreport@ar.be, limiting the information communicated to that necessary to understand and manage the situation. Automation & Robotics shall, under its own responsibility, assess and manage any obligations incumbent upon it under the applicable data protection regulations.
- The participant shall not retain any personal data beyond the period strictly necessary for the identification, documentation and reporting of the vulnerability. When retention is no longer necessary for these purposes, the participant shall delete such data or render it irreversibly unusable as soon as possible.
- The participant shall document, to the extent necessary for the traceability of its research and the handling of the report, the relevant operations it has carried out as well as any personal data to which it may have accessed incidentally. Such documentation shall be limited to what is necessary for the research, demonstration and reporting of the vulnerability.
- The participant may work with a third party to carry out its research. The participant must ensure that the third party first becomes aware of this policy and agrees, by providing assistance, to comply with its conditions, including confidentiality and the implementation of appropriate security measures. The participant remains responsible for compliance with this policy by the third parties it engages and shall ensure that such third parties comply with the obligations applicable to them, particularly with regard to confidentiality and security.
- The participant independently determines the technical means it uses to conduct its research and remains responsible for the processing of personal data it carries out on its own initiative and for its own purposes. Any potential and incidental access to personal data within the framework of this CVDP does not, in itself, make the participant a processor of Automation & Robotics.

This policy does not constitute a data processing agreement within the meaning of Article 28 of the GDPR. The participant acts independently and is not entrusted by A Automation & Robotics with processing personal data on its behalf.

3. How to Report Security Vulnerabilities

a) Contact Point

Reports should primarily be sent to the following email address: vulnerabilityreport@ar.be and/or using the following online form: *Indiquer le lien vers le formulaire*

Any personal data that may be collected as part of the handling of vulnerability reports is processed in accordance with the applicable regulations on the protection of personal data.

The personal data protection policy is also available at the following address: Privacy Policy - draft.pdf *(lien à ajouter)*

Tel: +32 (0)87 322 323
Email :
www.ar.be

Automation & Robotics S.A.
P. Industriel de Lambermont,
Rue des Ormes, 111 – 4800 Verviers - Belgium

TVA : BE0423637107
Verviers

b) Information to be Provided

As soon as possible after discovery, please send us information about your findings using the form provided in Annex I or the online form available here: *(url du formulaire)*

4. Procedure

a) Discovery

When a participant discovers information relating to a potential vulnerability, the participant should, where possible, first carry out checks to confirm the existence of the vulnerability and identify any potential risks.

b) Notification

The participant undertakes to notify, as soon as possible, any suspected or identified vulnerability, together with the available technical information enabling its analysis, via the point of contact defined in section 3 a) of this policy. The participant shall use the secure communication channels made available by Automation & Robotics.

Upon receipt of a report, Automation & Robotics undertakes to send the participant, as soon as possible, an acknowledgement of receipt indicating, where possible, the internal reference associated with the report, a reminder of the main obligations applicable under this Coordinated Vulnerability Disclosure Policy (CVDP), as well as the next steps in the handling process.

Where a report is likely to concern an actively exploited vulnerability or a serious incident affecting the security of a product with digital elements, the Product Security Incident Response Team (PSIRT) shall immediately initiate the applicable internal assessment procedure in order to determine the necessary measures and, where applicable, the regulatory notifications required under the Cyber Resilience Act.

Where a report reveals or raises suspicion of a personal data breach, the PSIRT shall immediately inform the person or internal function designated by Automation & Robotics to monitor matters relating to the protection of personal data. Automation & Robotics shall then, under its own responsibility, assess the breach and determine whether notification to the competent supervisory authority is required under the GDPR. Where such notification is required, it shall be made within the applicable legal deadlines and in accordance with the procedures prescribed by the Data Protection Authority.

c) Communication

Tel: +32 (0)87 322 323
Email :
www.ar.be

Automation & Robotics S.A.
P. Industriel de Lambermont,
Rue des Ormes, 111 – 4800 Verviers - Belgium

TVA : BE0423637107
Verviers

The parties undertake to make every effort to ensure continuous and effective communication. The information provided by the participant may indeed prove very useful in identifying the vulnerability and resolving it.

In the absence of a response from either party within the coordinated vulnerability disclosure process beyond a reasonable period, the parties may call upon the Centre for Cybersecurity Belgium (CCB) (vulnerabilityreport@cert.be), as the default coordinator, in accordance with the applicable coordination mechanisms and, where necessary, following coordination with Automation & Robotics, unless otherwise required by law.

d) Investigation

The investigation phase will enable Automation & Robotics to reproduce the reported environment and behavior in order to verify the information provided.

Automation & Robotics undertakes to regularly keep the participant informed of the results of the investigations and the actions taken following its notification.

During this process, the parties shall ensure that links are established with similar or related notifications, assess the risk and severity of the vulnerability and determine any other products or systems affected.

e) Development of a solution

The objective of the disclosure policy is to enable the development of a solution in order to eliminate the identified vulnerability before any damage is caused.

Taking into account the state of knowledge, implementation costs, severity and exploitability of the vulnerability, risks to users and technical constraints, Automation & Robotics will endeavor to develop and make available a solution within a target period of 90 calendar days. This period may be shortened when a critical or actively exploited vulnerability requires urgent action, or adjusted when specific technical constraints justify it.

During this phase, Automation & Robotics and its partners undertake to carry out, on the one hand, positive tests to verify that the solution works correctly and, on the other hand, negative tests to ensure that the solution does not disrupt the proper functioning of other existing functionalities.

f) Public disclosure

Automation & Robotics will decide, in coordination with the participant, on the arrangements for potentially making the existence of the vulnerability public. Where applicable, the existence of the vulnerability may be publicly disclosed, according to arrangements determined in coordination with the participant. Such public disclosure may not take place before a solution has Automation & Robotics deployed and a security advisory intended for users has Automation & Roboticsn issued, unless otherwise required by law or regulation.

Tel: +32 (0)87 322 323
Email :
www.ar.be

Automation & Robotics S.A.
P. Industriel de Lambermont,
Rue des Ormes, 111 – 4800 Verviers - Belgium

TVA : BE0423637107
Verviers

In the event of a vulnerability that also concerns other organizations, the responsible organization must, in any event, inform the Centre for Cybersecurity Belgium (vulnerabilityreport@cert.be), even if it does not wish the vulnerability to be publicly disclosed.

Automation & Robotics also undertakes to collect user feedback on the deployment of the solution and to take the necessary corrective measures to address any issues caused by the solution, particularly compatibility issues with other products or services.

5. Applicable Low

Belgian law shall apply to disputes relating to the application of this policy.

The CCB (vulnerabilityreport@cert.be) may act as an intermediary in an attempt to reconcile Automation & Robotics and the participant with regard to issues relating to the application of this policy.

6. Duration

The rules of this policy shall apply from 11/09/2026 until their possible amendment or removal by Automation & Robotics . Such amendments or removals shall be published on Automation & Robotics 's website and shall automatically apply 30 days after their publication.

Tel: +32 (0)87 322 323
Email :
www.ar.be

Automation & Robotics S.A.
P. Industriel de Lambermont,
Rue des Ormes, 111 – 4800 Verviers - Belgium

TVA : BE0423637107
Verviers