marelec

A DURAVANT COMPANY

# COORDINATED VULNERABILITY DISCLOSURE POLICY

HOW TO REPORT A SECURITY VULNERABILITY IN A MARELEC PRODUCT

26 AUGUST 2026
REVISION V1.0

**MARELEC Food Technologies**
Westendelaan 1 | 8620 Nieuwpoort | Belgium | T +32 58 222 111 | info@marelec.com | www.marelec.com
BTW/TVA/VAT BE-0554.865.932 | BNP Paribas Fortis BIC/Swift : GEBABEBB | IBAN BE73 0016 2313 6160 | RPR/RPM Veurne

## 1. OUR COMMITMENT

MARELEC Food Technologies designs and manufactures weighing, portioning, grading, batching and trawl control equipment, together with the embedded and desktop software that drives it. Many of these products contain digital elements and are connected to customer networks.

We take the security of our products seriously, but no product is free of vulnerabilities. We therefore welcome reports from security researchers, customers, integrators, suppliers and anyone else who discovers a weakness in a Marelec product or service. This policy explains how to report such a weakness, what we ask of you, and what you can expect from us in return.

This policy is published in accordance with Annex I, Part II of Regulation (EU) 2024/2847 (the Cyber Resilience Act) and applies to Marelec as a manufacturer. It covers all Marelec product lines; there is no separate policy per product.

## 2. SCOPE

### 2.1. IN SCOPE

- All Marelec products with digital elements, including their embedded software, firmware, configuration tooling and remote support components. This covers the following product families:
  - **Machines:** Portio Z2.5, Portio B, Portio Z5, Portio Jet, Grader Z2.5, Trimline Z2.5, MXV, Batchers, Flowscale Z2.5, Ultra Batcher Z2.5, iVision.
  - **Systems:** Omega, Weighing Scales, Trawl Control.
  - **Software:** Matrix, Matrix Pro.
- Internet-facing services operated by Marelec, including our websites and customer portals.
- Products that are discontinued or nearing discontinuation. We still want to know about vulnerabilities in them, but we may be limited in the remediation we can offer and may respond with mitigation guidance or an end-of-support statement instead of a fix.

### 2.2. OUT OF SCOPE

- Third-party products and services that Marelec does not develop or operate. Please report those to the responsible vendor. If a Marelec product ships or depends on the affected component, tell us as well so that we can assess the impact on our customers.
- Installations that have been modified by the customer or a third party in a way that is not part of the product as delivered.
- Mechanical, electrical or food safety concerns. Please raise those through your usual Marelec service contact so they reach the right team immediately.

### 2.3. REPORTS WE GENERALLY CANNOT ACT ON

- Denial-of-service, volumetric or resource-exhaustion testing of any kind.
- Phishing, spam, and mail configuration findings (SPF, DKIM, DMARC) without demonstrable impact.

- Social engineering of Marelec employees, customers or suppliers.
- Physical attacks against Marelec premises, staff or equipment.
- Raw output of automated scanners without a validated, demonstrated impact.
- Missing hardening measures, such as HTTP security headers or TLS configuration preferences, where no concrete exploitation path is shown.

## 3. HOW TO REPORT

| Channel | Details |
|---|---|
| Web form | marelec.com/security – our preferred channel. Submissions are delivered directly to our security mailbox. |
| E-mail | security-reporting@marelec.com – monitored by the Marelec product security team. |

Please do not report security issues through sales representatives, service technicians, social media or public issue trackers. Those channels are not monitored for security reports and public posts put other customers at risk.

We accept reports in English. You may report anonymously, but we will then be unable to ask follow-up questions or keep you informed.

## 4. REPORTING TO THE BELGIAN AUTHORITIES AS WELL

Belgian law offers you a second route, independent of this policy. Under the Law of 26 April 2024 any person acting without fraudulent or malicious intent may report a potential vulnerability in an ICT product or service located in Belgium to the Centre for Cybersecurity Belgium (CCB), the national CSIRT. Reports go to vulnerabilityreport@ccb.belgium.be using the notification forms published at ccb.belgium.be.

That procedure gives you protection under Belgian criminal and civil law, provided you meet the conditions the CCB sets. Those conditions include notifying **both** the organisation concerned and the CCB, with a simplified notification within 24 hours and a complete notification within 72 hours of discovery, and not disclosing the vulnerability publicly without the CCB's prior agreement.

We would rather hear from you first, so that we can begin work immediately, but using the legal procedure alongside this policy costs you nothing with us and we will not treat it as a breach of good faith. Where the CCB coordinates a report concerning a Marelec product, we cooperate with it.

## 5. WHAT TO INCLUDE IN YOUR REPORT

The more of the following you can provide, the faster we can act:

1. The affected product family, model and serial number, or the URL of the affected service.
2. The software, firmware or build version, where known.
3. A clear description of the vulnerability and the impact you believe it has.

4. Step-by-step instructions to reproduce it, including any proof-of-concept code, requests, scripts or screenshots.
5. The setup in which you found it: network configuration, connected systems, user privileges used.
6. Whether the issue is already publicly known, or whether you have any indication that it is being exploited.
7. How you would like to be credited if we publish an advisory, and how we can contact you.

## 6. WHAT HAPPENS NEXT

1. **Acknowledgement.** We confirm receipt of your report within five business days.
2. **Triage.** We register the report, assign a single point of contact, and route it to the product owner responsible for the affected product family.
3. **Validation and assessment.** We attempt to reproduce the issue and assess its severity, taking into account the impact on our customers' operations and on safety.
4. **Feedback.** We let you know whether we have accepted the report, whether it duplicates a known issue, or why we consider it out of scope, and we keep you informed at reasonable intervals while we work on it.
5. **Remediation.** We develop and test a fix or a mitigation. We do not commit to a fixed remediation deadline: our products run in production food processing lines and on vessels at sea, and updates must be validated so that they cannot compromise safe operation. We prioritise by risk, and we tell you what we are doing.
6. **Disclosure.** Once a fix or mitigation is available, we inform affected customers and, where appropriate, publish an advisory. We will agree the timing with you where possible and credit you if you wish. We ask you not to disclose details publicly before that moment.
7. **Regulatory notification.** Where the law requires it, in particular for actively exploited vulnerabilities under Article 14 of the Cyber Resilience Act, we notify the CSIRT designated as coordinator for Belgium, the Centre for Cybersecurity Belgium, and ENISA within the prescribed deadlines. Marelec is established in Belgium, and these notifications are filed once through the Single Reporting Platform operated by ENISA. This is independent of the disclosure timing agreed with you.

## 7. SAFE HARBOUR

If you make a good-faith effort to comply with this policy while researching and reporting a vulnerability, Marelec will not initiate legal action against you in relation to that research, and will treat your activity as authorised.

Acting in good faith means, at a minimum, that you:

- test only against systems and installations that you own or for which you have the explicit permission of the owner. Marelec machines are installed at our customers' premises and on their vessels; this policy does not give you permission to test them;
- do not access, modify, delete or copy more data than is strictly necessary to demonstrate the vulnerability, and do not access personal data belonging to others;
- do not disrupt, degrade or interrupt any production process, service or vessel operation;

- do not install backdoors, malware or persistence mechanisms, and remove any test artefacts;
- do not disclose the vulnerability publicly or to third parties before it has been resolved and the timing has been coordinated with us and, where you also use the Belgian legal reporting procedure, with the CCB;
- comply with applicable law.

Marelec can only speak for itself. This safe harbour does not bind our customers, our suppliers or any other third party, and it does not override any statutory obligation we have.

## 8. NO BUG BOUNTY

Marelec does not operate a bug bounty programme and does not offer monetary rewards, gifts or compensation for vulnerability reports. With your permission we will credit you by name or handle in the advisory we publish. We appreciate your work regardless.

## 9. CHANGES TO THIS POLICY

This policy may be updated. The current version is always available at marelec.com/security the version and date on the cover page indicate which revision you are reading. Product manuals refer to that address rather than to a specific revision.

## 10. REVISION HISTORY

| Version | Date | Change |
|---|---|---|
| v1.0 | 26 August 2026 | First version, prepared for internal review. Not published. |