rotork®

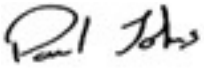
Keeping the World Flowing
for Future Generations

# Vulnerability Disclosure Policy

Cybersecurity ISMS document

## Revision Control

### Revision Approval

| Prepared by: | Checked by: | Approved by: |
|---|---|---|
| Product Cyber Security Engineer | Engineering Manager | Global Head of Cybersecurity / CISO |
| Name: Anjan Neema | Name: Paul Johns | Name: James Blannin |
| Sign: | Sign:  | Sign: |

### Revision(s) Summary

| Revision | Date | Summary |
|---|---|---|
| DRAFT 0.1 | 13/03/2026 | First draft |
| DRAFT 0.2 | 18/03/2026 | Second draft – Rotork ISMS policy template applied for INTERNAL copy |
| DRAFT 0.3 | 15/05/2026 | Third draft – Technical review comments addressed |
| Final Version 1.0 | 10/09/2026 | Closed all the open comments via the legal team |

### Next Review Date

| Date |
|---|
| TBD |

## Contents


1. Document Control 03
   - 1.1 Document Control Statement 03
   - 1.2 Document Classification, storage, and handling 03
   - 1.3 Distribution and Maintenance 03
2. Introduction 03
3. Purpose 03
4. Scope 03
5. Definitions 04
6. Reporting a Vulnerability 05
   - 6.1 Reporting Channel 05
   - 6.2 Information to Include 05
   - 6.3 Acknowledgement 05
7. Coordinated Vulnerability Disclosure Process 05
   - 7.1 Intake and Validation 05
   - 7.2 Risk and Severity Assessment 05
   - 7.3 Remediation 05
   - 7.4 Coordination with Reporter 05
   - 7.5 Public Disclosure 06
   - 7.6 Mandatory Reporting Obligations 06
8. Vulnerability Handling and Remediation 06
9. Security Updates and Advisories 06
10. Safe Harbour 06
11. Rules of Engagement for Security Researchers 07
12. Record Keeping and Traceability 07
13. Integration with Security Processes 07
14. Policy Maintenance 07
15. Contact Information 07


The name Rotork is a registered trademark. Rotork recognises all registered trademarks. Published and produced in the UK. POLTG1026. © Rotork 2026 all rights reserved. Rotork reserves the right to amend and change specifications without prior notice. For the latest version visit rotork.com

## 1. Document Control

### 1.1 Document Control Statement

This document is the property of Rotork. It shall not be reproduced wholly or in part without the permission of the Global Head of Cyber Security. Controlled copies will be issued and/or explained to any person(s) carrying out work on behalf of Rotork and can only be obtained from:

Rotork plc, Brassmill Lane, Bath, UK.

All controlled copies must be reviewed and updated in a timely manner.

### 1.2 Document Classification, storage, and handling

This document is intended for public distribution and may be shared externally. It has been prepared to provide information to customers, partners, suppliers, regulators, and other interested parties. Users should ensure they are referencing the latest published version, as the content may be updated periodically.

### 1.3 Distribution and Maintenance

It is required that this policy and its supporting standards and guidelines serve as an overarching guide for related cybersecurity processes and procedures within Rotork and that there are on-going review and maintenance. All approved changes and new releases of this document shall be made available to the persons concerned. The distribution and maintenance responsibility of the document shall be with the Information Security Officer.

## 2. Introduction

We are committed to ensuring the security, safety, reliability and availability of our products [and services] throughout their lifecycle and to handling reported vulnerabilities in a timely and responsible manner in line with applicable cybersecurity regulations and internationally recognised standards including the Cyber Resilience Act (Regulation (EU) 2024/2847 (hereinafter referred to as the 'CRA') .

## 3. Purpose

The purpose of this Vulnerability Disclosure Policy (VDP) is to provide a clear and structured process for external parties to report potential security Vulnerabilities affecting our industrial automation and control systems (IACS) Products as well as for how Rotork will receive, assess, remediate, remedy, report and publicly disclose fixed Vulnerabilities, and how it will fulfil its mandatory notification obligations to ENISA and the relevant CSIRT coordinator under Article 14 of the CRA.

## 4. Scope

This policy applies to all Products developed and manufactured by Rotork (where Rotork is the 'Economic Operator' or 'Manufacturer' of a Product that is Placed on the Market or Made Available on the Market , including:

- Industrial control and automation systems which are comprised of Products
- Embedded Product devices and controllers
- Software applications and firmware with digital elements
- Remote Data Processing solutions supporting these Products
- The following are explicitly out of scope:
- Third-party products or services not developed or maintained by Rotork
- Rotork's internal systems and infrastructure that are not Placed on the Market as Products or services for third parties are out of scope and must not be accessed or tested without explicit written authorisation from Rotork management.
- Any additional services not otherwise specified above.

## 5. Definitions

| Term | Definition | CRA Reference |
|---|---|---|
| Computer Security Incident Response Team (CSIRT) | The EU Member State agency responsible for coordinating cybersecurity incident response at the national and common market level. | N/A |
| Coordinated Vulnerability Disclosure (CVD) | A process where Vulnerabilities are reported privately and disclosed publicly after remediation is available | Annex I Part II (5) |
| Economic Operator | Means the manufacturer, the authorised representative, the importer, the distributor, or other natural or legal person who is subject to obligations in relation to the manufacture of Products or to the Making Available on the Market of Products in accordance with the CRA. | Article 3 (12) |
| European Network and Information Security Agency (ENISA) | The European Union Agency for Cybersecurity, responsible for strengthening cybersecurity across the EU. | N/A |
| Exploitable Vulnerability | Means a Vulnerability that has the potential to be effectively used by an adversary under practical operational conditions | Article 3 (40) |
| Made available on the Market | Means the supply of a Product for distribution or use on the EU market during a commercial activity, whether in return for payment or free of charge | Article 3 (22) |
| Manufacturer | Means a natural or legal person who develops or manufactures Products or has Products designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge | Article 3 (13) |
| Placed on the Market | Means making a Product available on the European Union market for the first time within the meaning of EU products law. Please note that this definition is distinct from the legislative term "Made available on the Market" referred to in the CRA Article 3(22) | Article 3 (21) |
| Product | Means a software or hardware product with digital elements and its Remote Data Processing solutions, including software or hardware components being Placed on the Market separately | Article 3 (1) |
| Product Security Incident Response Team (PSIRT) | PSIRT is the dedicated team within Rotork that receives, investigates, and coordinates responses to security incidents in the company's products, managing the full process from intake to disclosure. | N/A |
| Remote Data Processing | Means data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the Product from performing one of its functions | Article 3 (2) |
| Security Researcher | Any individual or organisation reporting a Vulnerability in good faith | N/A |
| Security Update | A patch or update that addresses one or more Vulnerabilities in a Product | Annex I Part II (8) |
| Single Reporting Platform (SRP) | The electronic platform operated and maintained by ENISA in accordance with EU CRA Article 16. | Article 16 |
| Software Bill of Materials (SBOM) | Means a formal record containing details and supply chain relationships of components included in the software elements of a Product | Article 3 (39) |
| Support Period | Means the period during which a manufacturer is required to ensure that Vulnerabilities of a Product are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I | Article 3 (20)<br>Annex I Part II |
| Vulnerability | Means a weakness, susceptibility or flaw of a Product that can be exploited by a cyber threat | Article 3 (40) |

For additional definitions, refer to the CRA Article 3 – Definitions.

## 6. Reporting a Vulnerability

We encourage responsible disclosure of Vulnerabilities.

### 6.1 Reporting Channel

Please report Vulnerabilities via one of the following:

- Email: psirt@rotork.com

All channels are monitored by the Product Security Incident Response Team, who acts as Rotork's single point of contact for vulnerability reporting in accordance with Article 13(17) of the CRA.

### 6.2 Information to Include

To help us assess the Vulnerability, please provide:

- Product name, version, serial number (if applicable), Product type (as shown on name plate, if applicable), and list all firmware versions installed on the Product, including updates.
- Description of the Vulnerability
- Steps to reproduce the exploitation of the Vulnerability
- Proof of concept or supporting material (if available)
- Potential impact assessment (if known)
- Description of mitigations already implemented (if known)
- Contact details for the person reporting the Vulnerability including: first name, last name, and email address. This is so that Rotork may gather additional information for its investigation and coordinate responsible Vulnerability disclosure.

* Anonymous reports are accepted, though Rotork's ability to follow up and coordinate disclosure may be limited where no contact details are provided.

### 6.3 Acknowledgement

Where contact details for the person reporting the Vulnerability have been provided:

- The Rotork PSIRT aims to acknowledge receipt of Vulnerability reports within 3 UK working days (being a day other than a Saturday, Sunday or Bank Holiday in London, England).
- The Rotork PSIRT may contact you for additional information if needed

## 7. Coordinated Vulnerability Disclosure Process

We follow a structured Coordinated Vulnerability Disclosure process:

### 7.1 Intake and Validation

- We will assess the applicability of the reported Vulnerability to our Products
- We will review and validate the reported Vulnerability
- We will confirm the scope and affected Products
- We will inform the reporter of the Vulnerability of the finding of our intake and validation process within 3 working days as defined above (where contact details for the person reporting the Vulnerability have been provided)

### 7.2 Risk and Severity Assessment

If the Vulnerability report is validated:

- We will assess the severity of the vulnerability using a recognised methodology
- We will evaluate the potential impact on the safety, availability, and operations particularly for IACS of end-users of Rotork Products
- We will assess whether the Vulnerability is an Exploitable Vulnerability
- We will determine whether the Vulnerability is an Actively Exploited Vulnerability. If so, the process will escalate immediately to Section 7.6 and the 24-hour reporting clock will be treated as running from the point of that determination.

### 7.3 Remediation

- We will prioritise addressing Vulnerabilities on a risk and operational impact basis
- We will develop and test risk mitigations and/or security updates as appropriate to the Vulnerability
- Risk mitigation advisories and security updates will be communicated to affected end-customers

### 7.4 Coordination with Reporter

- Where appropriate we may l agree on a disclosure timeline with the reporter of the Vulnerability
- Where appropriate we may will maintain communication with the reporter throughout our Vulnerability handling process

### 7.5 Public Disclosure

Where appropriate:

- We may publish a security advisory once a fix or mitigation is made available
- We may credit the reporter with the discovery of the Vulnerability where appropriate
- Under CRA Annex I Part II (4), we reserve the right to delay making public certain information regarding a fixed Vulnerability until after users have been given the possibility to apply the relevant remediation

### 7.6 Mandatory Reporting Obligations

If the Vulnerability report is found to be an Actively Exploited Vulnerability:

- We will issue an Early Warning Notification to ENISA and the appropriate coordinating CSIRT through the Single Reporting Platform, within 24 hours of becoming aware of an Actively Exploited Vulnerability, in compliance with CRA Article 14 requirements.
- We will issue a Vulnerability Notification to ENISA and the appropriate coordinating CSIRT through the Single Reporting Platform, within 72 hours of becoming aware of an Actively Exploited Vulnerability", in compliance with CRA Article 14 requirements.
- Unless relevant information has already been provided, we will issue a Final Report within 14 days after a corrective or mitigating measure is available, in compliance with CRA Article 14 requirements.

## 8. Vulnerability Handling and Remediation

We are committed to:

- Addressing and remediating Vulnerabilities without undue delay
- Providing security updates for Products during their defined support periods
- Coordinating with suppliers where Vulnerabilities affect third-party components (including by notifying the manufacturer or maintainer of that component without undue delay, and sharing relevant software or hardware modification developed by Rotork to address the Vulnerability)
- Reporting Vulnerabilities identified in integrated third-party components to the component manufacturer or maintainer and sharing any relevant fix in machine-readable format where appropriate
- Minimising disruption to operational environments, especially in safety-critical IACS deployments

Where immediate remediation is not possible, we will provide mitigation guidance.

## 9. Security Updates and Advisories

When Vulnerabilities are resolved, we will:

- Publish a security advisory on the www.rotork.com/en/eu-cyber-resilience-act including:
  - Description of the Vulnerability
  - Affected Products and versions
  - Severity rating
  - Remediation steps and/or workarounds
- Provide security updates free of charge and separately from functionality updates where technically feasible
- Ensure updates are distributed securely

Where applicable, users will be notified through available product interfaces and communication channels.

## 10. Safe Harbour

We will not directly pursue legal action against Security Researchers who:

- Act in good faith; and
- Follow this policy; and
- Avoid actions that could harm users, systems or data; and
- Do not break the applicable laws and regulations in the relevant legal jurisdictions*.

This includes refraining from:

- Exploiting Vulnerabilities beyond demonstrating a proof-of-concept
- Accessing or modifying end-user systems and data
- Disrupting operational systems
- Exploiting Vulnerabilities without explicit authorisation from the owner of the target systems or equipment

* For the avoidance of doubt, Rotork does not purport or intend by this clause to override applicable laws of relevant jurisdictions which may impose strict liability or where their good faith actions have caused an inadvertent breach of a relevant law. Rotork's intention under this clause is to clarify that, provided that the Security Research has acted in good faith, within the spirit of this policy Rotork will not initiate or directly cooperate with civil proceedings against the Security Researchers in relation to such actions.

## 11. Rules of Engagement for Security Researchers

Security researchers are expected to:

- Test only within the defined scope
- Avoid impacting system safety, availability, integrity and confidentiality, especially in operational industrial environments (including but not limited to intentional and accidental Denial-of-Service attacks and deploying malicious software)
- Not publicly disclose vulnerabilities before coordinated disclosure is complete
- Provide sufficient information to reproduce the issue when reporting a vulnerability

## 12. Record Keeping and Traceability

We maintain records in accordance with our record retention procedures of:

- Reported Vulnerabilities
- Assessment and remediation actions
- Communication with reporters of Vulnerabilities
- Disclosure timelines for validated Vulnerabilities

These records support compliance, auditability and continuous improvement of our security processes.

## 13. Integration with Security Processes

This policy is part of our broader product cybersecurity framework (and operates as a companion instrument to Rotork's Secure Development Policy), which includes:

- Secure development lifecycle practices
- Risk assessment and threat modelling
- Patch and security update management
- Product Security Incident Response Processes
- Supply chain cybersecurity management

## 14. Policy Maintenance

This policy is reviewed periodically and updated as necessary to reflect:

- Changes in regulatory requirements
- Evolving cyber threat landscape
- Improvements in internal processes

## 15. Contact Information

For Vulnerability reporting and enquiries:

- Email: psirt@rotork.com

Rotork appreciates the efforts of the security community in helping improve the security and resilience of our industrial automation and control system products and services.

rotork®

**Contact us now**

mail@rotork.com
www.rotork.com

PUB000-428-00
Issue 09/26