

data : 07/01/2026

Vulnerability Disclosure Policy – Ducati Energia S.p.A.

Purpose

The security of our products and services is a top priority for Ducati Energia S.p.A. and for our customers. For this reason, we promote a responsible and coordinated approach to vulnerability management, encouraging the reporting of potential issues and ensuring a transparent and secure process for their handling.

1. Vulnerability Reporting

Anyone outside the organization who identifies a potential vulnerability in Ducati Energia products or services must follow the official reporting procedure:

1. Submit the report by email to: it-security@ducatienergia.com
2. Provide sufficient information to enable assessment of the issue, including:
 - o Name and contact details of the reporter
 - o Date and method by which the vulnerability was identified
 - o Technical description of the vulnerability, including product/service, version, and configuration
 - o Any proof of concept or test code (clearly marked)
 - o Risk assessment or evidence of exploitation of the vulnerability

2. Management and Assessment

Ducati Energia commits to:

- Acknowledging receipt of the report within 7 business days and assigning a unique tracking ID.
- Assigning an internal point of contact to manage the case.
- Involving the relevant technical teams to assess and validate the vulnerability.
- If necessary, forwarding the report to third-party suppliers and informing you of the actions taken (subject to your consent to share your details).
- Keeping you informed of the status of the report until full resolution.



3. Mitigation and Remediation

Ducati Energia will:

- Verify the vulnerability and confirm its actual existence.
- Develop and test any required fixes.
- Perform internal validation (QA) prior to releasing the fix.
- Release updates or patches in accordance with customer notification processes.
- Share lessons learned with development teams to help prevent future vulnerabilities.

4. Acknowledgement and Transparency

Information received during responsible disclosure will be considered non-proprietary and may be used by the company to improve the security of its products and services.

Head of Technical Office
Enrico Girardi, Engineer

