Company FPT Industrial		Cybersecurity Coordinated Vulnerability Disclosure Policy	
Function Technical Certification and Compliance	**Version** **1.0**	**Date:** 03/09/2026	**Page:** 1/5

1 PURPOSE

FPT Industrial is committed to the timely identification, assessment, remediation and coordinated disclosure of cybersecurity vulnerabilities affecting products with digital elements.

This policy defines the principles governing the reception, handling, sharing and disclosure of vulnerability information in accordance with applicable regulatory requirements, including Regulation (EU) 2024/2847 (Cyber Resilience Act).

2 SCOPE

This policy applies to cybersecurity vulnerabilities affecting FPT products:

- Electronic Control Units (ECUs)
- Embedded Software
- Diagnostic Services
- Communication Interfaces
- Connected Services and devices
- Development and Maintenance Tools
- Third-party software and components integrated into FPT products

3 VULNERABILITY REPORTING

Vulnerabilities may be reported by:

- Customers (OEMs)
- Suppliers
- Security researchers
- Threat intelligence feeds
- Internal personnel
- Others

Reports shall be submitted through the cybersecurity reporting channel established by FPT.

3.1 Reporting Channels

To report a vulnerability or cybersecurity incident involving a FPT product, please notify to e-mail address**:** **FPT-CyberVulnerability@ivecogroup.com**

Please include the following in your report:

- Email subject line: “Potential Vulnerability”
- Product, model, version
- Description of the concern or vulnerability - include CVE where applicable
- Information to help our team replicate the issue (e.g. configuration details)
- Contact information

3.2 What We Expect

External reporters notifying vulnerabilities are asked to:

- Not disclose the vulnerability publicly if not agreed with FPT
- Not exfiltrate or destroy any data
- Not conduct denial-of-service attacks
- Agree on a timeframe for remediation

4 VULNERABILITY HANDLING PRINCIPLES

4.1 Receive and acknowledge vulnerability reports

All reported vulnerabilities shall be registered and assessed by FPT

4.2 Validate reported vulnerabilities

FPT shall determine:
- validity of the reported issue;
- affected products and versions;
- potential impact;
- exploitability.

4.3 Assess cybersecurity risk

A cybersecurity assessment shall be performed using the applicable cybersecurity processes and methods.

4.4 Define remediation measures

Where appropriate, FPT shall:
- develop corrective actions;
- define mitigations;
- prepare software updates;
- determine deployment recommendations.

5 COORDINATION WITH CUSTOMERS

For products supplied to OEM customers, FPT adopts a coordinated vulnerability disclosure approach.
Information regarding validated vulnerabilities shall be shared with affected customers to support a joint evaluation of:
- affected vehicle populations;
- operational impact;
- cybersecurity risk;
- available mitigations;
- remediation strategy.

This coordinated approach enables affected parties to implement appropriate risk treatment measures before public disclosure.

6 COORDINATION WITH SUPPLIERS

FPT expects suppliers to promptly communicate vulnerabilities affecting components, software or services integrated into FPT products.
Suppliers should provide:
- vulnerability description;
- affected versions;
- severity assessment;
- mitigation options;
- remediation roadmap;
- disclosure constraints, if applicable.

FPT shall evaluate supplier-provided vulnerability information within its own cybersecurity risk management process.

7 COORDINATED DISCLOSURE

FPT supports responsible and coordinated disclosure of cybersecurity vulnerabilities.
Disclosure activities should take into consideration:

- availability of mitigations or fixes;
- potential risks of premature disclosure;
- coordination with affected customers;
- regulatory reporting obligations.

Public disclosure may be postponed when immediate publication could increase cybersecurity risks or facilitate exploitation.

8 SECURITY ADVISORY

When appropriate, FPT may issue a Security Advisory containing information necessary to support customer risk analysis and remediation planning.
The advisory should include:
Description: Description of the vulnerability.

Affected Products: Products, components and versions concerned.

Impact: Potential cybersecurity effects.

Severity: Severity assessment and risk classification.

Mitigations: Available temporary measures.

Remediation: Available software corrections or planned updates.

References: Relevant identifiers (e.g. CVE, CERT references).

9 JOINT RISK EVALUATION

For products delivered to OEM customers, vulnerability information is shared to enable a joint risk evaluation.
The evaluation may consider:

- technical exploitability;
- affected product configurations;
- operational context;
- existing security controls;
- remediation feasibility.

Results of this evaluation support decisions regarding remediation, deployment actions and customer communications.

10 REGULATORY REPORTING

Where required by applicable regulations, including the Cyber Resilience Act, FPT shall perform the necessary regulatory reporting activities through the processes defined in the applicable cybersecurity procedures.

11 CONFIDENTIALITY

Vulnerability information shall be treated as confidential and shared only with parties having a legitimate need to know, unless and until disclosure is authorized.

12 SAFE HARBOR

FPT Industrial will not take legal action against security researchers who:

- Act in good faith
- Comply with this Disclosure Policy
- Do not access, copy or destroy data without authorisation
- Do not impair services through denial-of-service
- Do not endanger affected third parties