Vulnerability Disclosure and Communication Policy

Department:	All	**Type:**	Policy
Applies To:	Global	**Last Reviewed:**	2 October 2026
Administrator:	Security Operations	**Last Approved:**	2 October 2026
Approver:	CISO	**Effective As:**	2026

1 Purpose

Powerfleet is committed to maintaining the security, integrity and resilience of its products and services. This Policy establishes the framework for reporting cybersecurity vulnerabilities to Powerfleet and for communicating vulnerability-related information to customers, users, partners, regulators and other stakeholders, where appropriate.

2 Scope

This Policy applies to cybersecurity vulnerabilities that may affect Powerfleet products, software, services, or supporting infrastructure.

3 Reporting Vulnerabilities to Powerfleet

3.1 Reporting Method

Powerfleet encourages customers, security researchers, suppliers, partners and other interested parties to report suspected cybersecurity vulnerabilities affecting Powerfleet products or services.

Vulnerability reports should be submitted to: privacy@powerfleet.com

Reporters are not required to provide their identity or other personal information when submitting a vulnerability report.

Powerfleet will acknowledge receipt of vulnerability reports within five working days and will maintain appropriate communication with the reporter during the assessment and handling of the report.

3.2 Reporter Confidentiality

Powerfleet will not publicly disclose the identity or contact details of a reporter without their consent, unless required by law.

3.3 Responsible Reporting

Powerfleet encourages vulnerability reports to be made responsibly and in a manner that minimises unnecessary risk to customers, users, systems and data.

Reporters are encouraged to allow Powerfleet a reasonable opportunity to assess and address the reported vulnerability before disclosing details publicly.

3.4 Good-Faith Reporting

Powerfleet values and encourages good-faith vulnerability reporting. Powerfleet will not act against a reporter solely for making a good-faith report of a suspected vulnerability.

Nothing in this Policy authorises testing or limits Powerfleet's rights in relation to unlawful, malicious or harmful activity.

3.5 Vulnerability Handling

Powerfleet maintains internal processes for identifying, assessing, prioritising, remediating and tracking cybersecurity vulnerabilities throughout their lifecycle.

4 Communication of Vulnerabilities by Powerfleet

4.1 Customer and Stakeholder Communications

Powerfleet is committed to communicating information about vulnerabilities, mitigations and remediation activities to affected customers and other appropriate stakeholders where such communication supports the protection of customer information, systems, services or operations.

Communications may be provided through security advisories, customer notifications, support communications, release notes or other appropriate channels.

4.2 Regulatory and Authority Notifications

Where required by applicable laws, regulations or contractual obligations, Powerfleet will provide information relating to vulnerabilities or associated cybersecurity events to the relevant regulators, competent authorities, computer security incident response teams or other authorised entities.

4.3 Public Disclosure

Powerfleet may publicly disclose information relating to vulnerabilities, and associated remediation activities where such disclosure supports customer protection, risk mitigation, security awareness, regulatory compliance or coordinated vulnerability disclosure.

The timing and content of any public disclosure will be informed by the need to protect affected parties, the availability of mitigations or corrective measures, and applicable legal and regulatory obligations.