

Vulnerability Disclosure Policy

Coordinated reporting and handling of security vulnerabilities affecting ESA systems and services

PUBLIC | APPROVED | Version 1.0 | 12 October 2026

1. Purpose and scope

Echelon Strategic Advisory (ESA) Limited (ESA) is committed to addressing and reporting security issues through a coordinated and constructive approach designed to protect our customers, partners, staff, associates and other users of our services.

A security vulnerability is a weakness in our systems or services that may compromise their security. This policy applies to security vulnerabilities discovered by ESA staff, associates, customers, suppliers, security researchers or other third parties. Responsibility for this policy rests with ESA senior management and it will be reviewed at least annually. Staff and associates must follow this policy and receive appropriate security awareness training.

2. Reporting vulnerabilities

HOW TO REPORT A VULNERABILITY

If you believe you have discovered a vulnerability in an ESA service, system or website, or have a security incident or suspected weakness to report, please email enquiries@esaglobal.co.uk with the subject "Security Vulnerability". Please include enough information for us to understand and investigate the issue. Staff and associates may also report concerns directly to Matt Moon or Greg Scott.

3. How ESA responds

Once ESA receives a vulnerability report, we will take proportionate steps to address the issue:

- We will acknowledge receipt of the report promptly.
- We will handle the report sensitively and ask the reporter to keep vulnerability details confidential while we investigate and remediate the issue.
- We will work with the reporter, where appropriate, to understand and investigate the vulnerability.
- We will provide a reasonable indication of the expected remediation timeframe where practicable.
- We will notify the reporter when the issue has been resolved, where appropriate, so that retesting can take place if needed.
- Where appropriate, ESA will coordinate any external disclosure after remediation, taking account of customer, legal, regulatory and security considerations.
- ESA will respect a reporter's preference to remain anonymous and will not identify a reporter publicly without their agreement.

ESA will endeavour to keep the reporter appropriately informed as the issue is investigated and resolved. Good-faith reports of security weaknesses will not result in retaliation, adverse treatment or recrimination. ESA does not intend to pursue legal action against researchers who act in good faith, stay within the scope of this policy and avoid harm to ESA, its customers or third parties.

4. Responsible reporting guidance

We appreciate the efforts of security researchers and others who responsibly share information about security issues with us. To help us investigate safely and effectively, we ask reporters to:

- Give ESA a reasonable opportunity to investigate and correct a vulnerability before publicly disclosing it.
- Provide sufficient detail to allow us to investigate, including steps to reproduce the issue where possible.
- Use the Common Vulnerability Scoring System (CVSS) when helpful, although this is not required.
- Avoid modifying or deleting data, disrupting services, accessing unnecessary information, or taking actions that could adversely affect ESA customers or third parties.
- Do not conduct social engineering, denial-of-service testing, physical security testing, or other intrusive activity without ESA's explicit prior written permission.

5. Document control and attribution

Document	Vulnerability Disclosure Policy
Version	1.0
Status	Approved
Policy owner	Matt Moon
Approval date	12 October 2026
Review by	12 October 2027

ESA adaptation approved for use: Version 1.0 | 12 October 2026 | Policy owner: Matt Moon | Review by: 12 October 2027

© The IASME Consortium Limited 2025

Adapted from The IASME Consortium Limited Vulnerability Disclosure Policy template (2025). Licensed under Creative Commons BY-SA 4.0: <https://creativecommons.org/licenses/by-sa/4.0/>. Changes made by Echelon Strategic Advisory (ESA) Limited. This adaptation is distributed under the same licence.