

Responsible Disclosure Policy

LAST UPDATED: 9 JULY 2026

How to report a potential security vulnerability in Revenant Systems websites, applications or services, and what to expect when you do.

1. Introduction

At Revenant Systems, we take the security of our software, services and users seriously.

We appreciate the efforts of security researchers, customers and members of the wider technology community who help identify potential security issues.

This Responsible Disclosure Policy explains how potential vulnerabilities can be reported to us.

2. Our Approach

Security is an ongoing process, and we recognise that external feedback can help identify issues that may not be discovered through normal development and testing activities.

We encourage responsible reporting of potential security vulnerabilities so that we can investigate and address them appropriately.

3. What to Report

Examples of issues that may be appropriate to report include:

- Security vulnerabilities in Revenant Systems websites or applications
- Unauthorised access issues
- Data exposure concerns
- Authentication or authorisation weaknesses
- Software vulnerabilities that could impact users

If you are unsure whether an issue is security-related, we encourage you to report it.

4. How to Report a Security Issue

Please provide as much information as possible, including:

- A description of the potential vulnerability
- The affected product, service or website
- Steps required to reproduce the issue
- Any relevant screenshots, logs or technical details
- Potential impact of the issue

Reports should be sent to:

Email: hello@revenantsystems.co.uk

5. Responsible Testing

When investigating or reporting potential vulnerabilities, we ask that researchers:

- Avoid accessing, modifying or deleting other users' information
- Avoid disrupting services or systems
- Avoid performing actions that could negatively impact availability
- Do not publicly disclose details of a vulnerability before we have had an opportunity to investigate and address it

Testing should be limited to identifying and demonstrating the potential issue.

6. Our Response

When we receive a security report, we will:

- Review the information provided
- Assess the potential impact
- Investigate where appropriate
- Take reasonable steps to address confirmed issues

The time required to investigate and resolve issues may vary depending on complexity, severity and available resources.

7. Scope

This policy applies to Revenant Systems services and products operated by Revenant Systems.

Some products developed by Revenant Systems may have additional security guidance or reporting processes.

8. Good Faith Reporting

We appreciate good faith security research.

Where someone follows this Responsible Disclosure Policy, we will consider the circumstances of the report and aim to work constructively towards resolving valid security concerns.

Where you make a genuine, good-faith effort to follow this policy, we will not pursue legal action against you in relation to your research.

This policy does not give permission to act unlawfully, and testing must stay within the limits described above.

We do not operate a paid bug bounty programme and cannot offer financial rewards for reports — but we are grateful for them, and we are happy to credit researchers who wish to be named.

QUESTIONS

If you have any questions about the Responsible Disclosure Policy, contact Revenant Systems Ltd at hello@revenantsystems.co.uk or visit <https://revenantsystems.co.uk>.