

Information Security Statement

LAST UPDATED: 8 JULY 2026

How Revenant Systems protects information and builds secure software — secure development practices, access management and vulnerability handling.

1. Our Commitment to Security

At Revenant Systems, we believe security is an essential part of building reliable software.

We aim to design and develop applications and technology solutions that are secure, maintainable and respectful of the information entrusted to us.

Security is considered throughout the software development lifecycle, from initial design through to deployment and ongoing improvement.

2. Our Approach

As a small UK software company, we take a practical and proportionate approach to information security.

Our security practices are designed around the principles of:

- Protecting confidentiality
- Maintaining integrity of information
- Supporting availability of services
- Reducing unnecessary risk

The specific security measures applied may vary depending on the technology, service and requirements involved.

3. Secure Development Practices

We aim to incorporate security considerations throughout our development process.

This includes:

- Considering security during application design
- Following recognised software development good practices
- Reviewing dependencies and third-party components

- Applying updates and security fixes where appropriate
- Avoiding unnecessary collection or processing of data
- Testing functionality and behaviour before release

4. Access Management

Access to systems and services is managed based on business requirements.

Where appropriate, we use:

- Strong authentication methods
- Multi-factor authentication
- Appropriate access restrictions
- Least privilege principles

Access is reviewed when changes occur to responsibilities or requirements.

5. Data Protection

We aim to protect personal and confidential information through appropriate safeguards.

Our approach includes:

- Minimising the information we collect
- Limiting access to information where possible
- Using secure systems and service providers
- Protecting information during storage and transmission where appropriate

Further information about personal data handling is available in our Privacy Policy and Data Protection & UK GDPR Statement.

6. Cloud and Third-Party Services

Where Revenant Systems uses cloud platforms, development tools or third-party services, we consider their suitability and security practices.

Third-party services may include:

- Cloud hosting providers
- Software development platforms
- Communication services
- Business tools

We aim to use reputable providers and configure services appropriately for their intended purpose.

7. Vulnerability Management

We recognise that software security requires ongoing attention.

Where potential vulnerabilities or security issues are identified, we aim to:

- Assess the potential impact
- Apply appropriate fixes or mitigations
- Update affected systems where practical
- Learn from issues to improve future development

Security concerns can also be reported through our Responsible Disclosure Policy.

8. Responsible Security Research

We welcome responsible reporting of potential security issues.

If you believe you have identified a security vulnerability affecting Revenant Systems services, please contact us with relevant details so that we can investigate appropriately.

9. Continuous Improvement

Security is an ongoing process.

As Revenant Systems grows, we will continue to review and improve our security practices, tooling and development approaches.

We aim to build software that customers can trust.

QUESTIONS

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