

Vulnerability Management Policy

Document control

ITEM	DETAIL
Organisation	InnoRail, Company No. 17055194, registered in England and Wales
Policy owner	Tim Jones, Chief Technology Officer and Security Lead
Version	1.0
Approved	Tim Jones, Chief Technology Officer, July 2026
Next review	July 2027, or sooner after a significant security incident or change to our services
Related documents	Data Protection Policy and Privacy Notice; service design documents for each customer service

1. Purpose, scope and standards

InnoRail ("InnoRail International") finds, assesses and fixes security vulnerabilities in a timely, consistent way, so that our products, the data they hold and our customers stay protected. This policy sets out how we do that and the timescales we work to.

It covers:

- the software products and services we provide to customers, including their code, third party components, cloud infrastructure and integrations;
- our corporate IT: laptops, mobile devices, email, collaboration tools and network equipment;
- everyone who works for or with us, including contractors and delivery partners with access to our systems.

We align to:

- the Cyber Essentials requirements for security update management;
- NCSC vulnerability management guidance and the NCSC Cloud Security Principles;
- the CIS Benchmarks and the AWS Well-Architected Framework (Security Pillar) for cloud configuration;
- the OWASP Top 10 and ISO/IEC 29147 and 30111 for vulnerability disclosure and handling.

2. Roles and responsibilities

ROLE	RESPONSIBILITY
Chief Technology Officer and Security Lead (Tim Jones)	Owns this policy; approves risk ratings, exceptions and emergency changes; reports to customers
Engineering lead and developers	Run scanning in the build pipeline, fix vulnerabilities in code and dependencies, retest fixes
Service Manager	Tracks vulnerabilities to closure against the target times; includes status in monthly service reports
All staff and contractors	Install updates promptly on their devices; report anything suspicious straight away

ROLE	RESPONSIBILITY
Suppliers and partners	Patch their own services and tell us about vulnerabilities that affect us

3. Identifying vulnerabilities

We use several sources, so that weaknesses are found by us before anyone else finds them:

SOURCE	WHAT IT COVERS	HOW OFTEN
Static code analysis (SAST) and secret scanning	Our own code	Every build
Dependency scanning against a software bill of materials (SBOM)	Third party libraries and packages	Every build, and daily against newly published vulnerabilities
Container image scanning	Base images and runtime packages	Every build, and continuously for images in use
Cloud security posture monitoring (AWS Security Hub, AWS Config, Amazon GuardDuty)	Cloud configuration against CIS and AWS best practice; threat detection	Continuous
External scanning	Public endpoints, including TLS configuration	At least monthly
Independent penetration testing by a CREST accredited provider	Applications, APIs and cloud configuration	At least annually, and after any significant change to the architecture
Device and software inventory checks	Staff laptops, mobile devices and software	Continuous, through device management
Threat intelligence	NCSC advisories, vendor security bulletins, CVE and CISA Known Exploited Vulnerabilities feeds	Reviewed weekly, and as alerts arrive
Reports from others	Customers, researchers and partners (section 6)	As received

Every vulnerability found is recorded in our tracking system with its source, affected assets, severity, owner and target date.

4. Assessing and fixing vulnerabilities

We rate each vulnerability using its CVSS v3.1 or v4.0 base score, then adjust for real world risk: whether it is being actively exploited, whether the affected component is reachable from the internet, and what data or service it could affect. The Security Lead approves the final rating.

The clock starts when the vulnerability is identified, or when a fix becomes available if none exists yet.

SEVERITY	CVSS SCORE	FIX WITHIN	NOTES
Critical	9.0 to 10.0	14 days	48 hours if actively exploited or on the CISA Known Exploited Vulnerabilities list. Handled as a P1 incident if a live service is at risk
High	7.0 to 8.9	14 days	Meets the Cyber Essentials requirement for high and critical updates
Medium	4.0 to 6.9	90 days	Normally included in a scheduled monthly release
Low	0.1 to 3.9	180 days	Fixed in a scheduled release, or risk accepted and recorded

Where a fix cannot be applied in time, we put temporary controls in place, such as a web application firewall rule, disabling the affected feature or restricting access, and record an exception (section 7). Every fix is retested before

the vulnerability is closed. Critical and high findings from penetration tests are confirmed fixed by the testing provider.

5. Patch management and secure deployment

- **Cloud services:** managed AWS services are patched by AWS. We update our own components (dependencies and base container images) at least monthly, and sooner to meet the target times in section 4.
- **Corporate devices and software:** operating systems and applications are set to update automatically. Security updates rated critical or high are installed within 14 days of release. Software that is no longer supported by its vendor is removed.
- **Testing:** every release, including security patches, passes our automated build checks and regression test suite before it goes live.
- **Deployment:** releases are applied by InnoRail International through an automated pipeline with no downtime and a tested rollback. Routine releases avoid customers' peak periods and are notified at least 5 business days in advance. Emergency security patches are applied as soon as practicable and the customer is told.
- **Records:** every patch and release is logged, so we can show what was applied, when, and by whom.

6. Reporting a security issue (responsible disclosure)

If you think you have found a security vulnerability in any InnoRail International product or service, please tell us.

- **Email:** security@innorail.co.uk
- **Include:** the product or web address affected, a description of the issue, steps to reproduce it, and your contact details.

What you can expect from us:

STEP	TIMESCALE
Acknowledge your report	Within 2 business days
Initial assessment and severity rating	Within 5 business days
Progress updates	At least every 14 days until resolved
Fix	Within the target times in section 4
Agree public disclosure with you	Once the fix is in place, normally within 90 days of your report

We ask you to act in good faith: do not access, change or delete data that is not yours; do not disrupt our services or attempt denial of service or social engineering; and give us reasonable time to fix the issue before telling anyone else. We will not take legal action against anyone who reports a vulnerability in good faith and in line with this policy. We will credit you, with your permission.

We publish a security.txt file on our website pointing to this route.

7. Exceptions

If a vulnerability cannot be fixed within its target time, for example because no fix exists yet or a fix would break a critical function, the owner records an exception with:

- the reason, and the risk of leaving it unfixed;
- the temporary controls in place;
- a new target date, no more than 90 days away.

The Security Lead must approve every exception. Exceptions for critical or high vulnerabilities in a customer's service are also shared with that customer. Exceptions are reviewed at least monthly until closed.

8. Telling customers and reporting

- Customers are told without undue delay about any critical or high vulnerability that affects their service, with the planned fix and any action they need to take.

- A vulnerability that has been exploited, or that has put customer data at risk, is handled as a security incident under our incident response process. Any personal data breach is reported under our Data Protection Policy.
- Each customer's monthly service report includes open vulnerabilities by severity, fixes applied, and performance against target times.
- Penetration test summaries are available to customers under a non-disclosure agreement.

9. Review

The Security Lead reviews this policy at least once a year, and after any significant security incident or change to our services. The latest version is always published on our website.