RESPONSIBLE DISCLOSURE POLICY

Scope

Ingersoll Rand takes the security of our products, services, and digital ecosystems seriously. We welcome reports of potential security vulnerabilities from anyone, including customers, distributors, system integrators, suppliers/technology partners, independent security researchers, and other members of the public.

This policy applies to cybersecurity vulnerabilities in products, components, software, firmware, cloud services, mobile apps, and web properties, including those marketed or operated by Ingersoll Rand and all subsidiary companies and brands. We accept reports regardless of product lifecycle status (including end-of-life), though remediation options for unsupported products may be limited.

The following are generally out of scope for this policy:

- Technical support requests (configuration help, feature requests, general troubleshooting)
- Issues in products/services where Ingersoll Rand is not responsible (e.g., third-party systems not operated by Ingersoll Rand)
- Purely informational findings without a clear security impact (may be deprioritized)

How to Report a Vulnerability

We provide a central reporting entry point via a dedicated web form on our Coordinated Vulnerability Disclosure (CVD) website.

If you are a customer, distributor, or partner and already have an account team or support contact, you may notify them in parallel. However, all technical details must be submitted through the official CVD channel to ensure the report is properly tracked and handled by our Product Security Incident Response Team (PSIRT).

Information to Include

To enable efficient analysis, validation, and remediation, please provide as much detail as possible in your submission. The web form will guide you, but at a minimum include:

- Affected product(s) or service(s), including version(s)
- Clear description of the vulnerability, including steps to reproduce the issue and required preconditions (if any)
- Expected vs. actual behavior
- Environment details, where relevant (e.g., configurations, operating system, network setup)
- Security impact, including potential effects on confidentiality, integrity, availability, and safety (if applicable)
- Proof-of-concept (PoC) or supporting material, limited to what is necessary to demonstrate the issue

For vulnerabilities that may be actively exploited, please include any available evidence, indicators of compromise, or observations that suggest ongoing exploitation.

We accept anonymous vulnerability reports. However, providing contact information is strongly encouraged, as it enables us to seek clarification, share status updates, and coordinate responsible disclosure. Anonymous submissions may limit our ability to effectively follow up.

Guidelines for Vulnerability Discovery and Testing (Rules)

We welcome reports from people who observe vulnerabilities during normal use and from people who actively test.

If you are actively testing (e.g., security research), please:

- Act in good faith and minimize impact
- Avoid privacy violations: do not access, copy, modify, retain, or disclose data that is not your own
- Avoid service disruption (no DoS, no destructive testing)
- Avoid high-volume automated scanning that could degrade services
- Stop testing once the issue is confirmed and report promptly
- Keep details confidential until coordinated disclosure

If you inadvertently access sensitive data, stop immediately, do not retain it, and report what happened so we can assess risk.

Safe Harbor (Non-Retaliation for Good-Faith Research)

If you discover and report a vulnerability in good faith and in accordance with this policy, Ingersoll Rand will not:

- pursue legal or civil action against you,
- report you to law enforcement, or
- terminate or restrict your access to our products/services solely because of your research.

This safe harbor applies provided you did not intentionally access data beyond your own, did not disrupt services, and reported to us before public disclosure.

In cases of non-compliance with these rules, Ingersoll Rand reserves the right to take appropriate action.

What You Can Expect from Us

Analysis: We will review and attempt to reproduce the reported vulnerability in line with our internal processes. We may request additional information and will keep you informed of progress. If confirmed, we will assess severity and potential impact.

Handling: For confirmed vulnerabilities, we will define and prioritize remediation or mitigation actions based on risk and impact. For end-of-life products, we may provide guidance where fixes are not feasible.

Disclosure: Following remediation or mitigation, we may publish a Security Advisory, balancing transparency with allowing customers time to apply fixes.

Third-Party Components and Multi-Party Coordination

If a reported issue is caused by a vulnerability in a generally available third-party product/service, we may coordinate with the upstream vendor and/or a coordination body to support remediation and responsible disclosure.

Recognition and Appreciation

Ingersoll Rand does not offer monetary rewards or public recognition programs for vulnerability reports.

However, we sincerely value the efforts of individuals and organizations who responsibly report vulnerabilities and contribute to improving the security of our products and services. Your collaboration helps us strengthen our overall security posture and better protect our customers.