Renishaw Group Vulnerability Disclosure Policy

Policy purpose and values

Renishaw is committed to delivering products that are secure.

Scope

This policy describes how you can report a vulnerability to us and how we will receive, investigate, and respond to reported vulnerabilities in our products, on our website, or otherwise affecting our corporate systems.

Policy statement

We welcome information about potential vulnerabilities to enable us to investigate and fix any issues as soon as possible.

We will investigate vulnerabilities and (if applicable) issue vulnerability advisory notices and security updates to eligible customers for commercially released products until such product, model, or version (as applicable) reaches its end of support date.

Policy

How to report a vulnerability

If you believe you have found a potential vulnerability, contact us via vulnerabilities@renishaw.com.

To help us to investigate efficiently, please provide relevant information in your report, including:

- Product name, model, version, or serial number (if applicable).
- Time and date of your discovery.
- Is this vulnerability being actively exploited?
- Detailed description (e.g. actions being performed, operating system, browser type and version, connected components and devices).
- Step-by-step instructions or sample code to demonstrate the vulnerability.
- Do you intend to report or disclose this vulnerability to any other parties (e.g. other affected vendors)?
- Your name and contact details, including your PGP key (optional).
- May we share your contact details with relevant third parties (e.g. affected vendors and security experts)?

You can use the Renishaw PGP public key and fingerprint 3712 78F3 9F7E FBF8 8047 032E 6B8C 4675 DC49 CED5 to encrypt your report.

If you have a query or request which is not related to vulnerability reporting, use our Contact us page instead.

Coordination with third parties

If we believe your reported vulnerability originates from a vendor or service provider, we will share the report with them to enable their own investigation and remediation efforts.

We may also notify and cooperate with security experts and relevant authorities when we become aware of vulnerabilities.

Timeline

We cannot commit to a set timeline for the investigation and remediation of a report, as this will depend on the nature, complexity, and severity of the case and whether we need to coordinate with third party vendors and service providers.

If you provide contact details with your report, we will acknowledge receipt within 2 days and keep you informed of progress until the report has been resolved or closed.

Disclosure

We ask that you do not publicly disclose details of the vulnerability without our prior agreement so that we have an opportunity to investigate and, where necessary, release a security update to protect our customers.

Vulnerability advisory notices

When it is appropriate to disclose details of a product vulnerability, we will issue a vulnerability advisory notice.

Depending on the severity of the product vulnerability, we may also attempt to contact customers directly (for example by telephone or email to a designated account contact).

Vulnerability advisory notices may require an update or other customer action. You are responsible for taking any recommended actions promptly to mitigate security risks for your product and environment.

Responsible testing

You must act in good faith and comply with all applicable laws and regulations in connection with security research activities and vulnerability reporting.

You must not:

- Use high-intensity invasive scanning tools to find vulnerabilities.
- Attempt any form of denial of service.
- Exploit any vulnerability beyond minimum testing to demonstrate it exists.
- Compromise, modify, corrupt, delete, or exfiltrate data.
- Attack, damage or disrupt systems or infrastructure.
- Use social engineering, phishing, or similar techniques.

Credit

We value responsible vulnerability reporting under this policy. However, we do not offer monetary rewards for vulnerability disclosures.

Upon mutual agreement, we may credit you for discovering the vulnerability in our advisory notice.

Privacy

We ask that you provide your name and contact details to facilitate further information sharing and to provide progress updates, but you may also submit your report anonymously. We process personal information in accordance with our privacy notice.

Policy number	Issue number	Change description	Effective date
BSP059	**01**	**First issue**	**19 May 2025**