

Document Number SEN0009	Revision 1.0	Prepared By NB	Approved By NGB
Title Senquip Vulnerability Disclosure Policy		Confidentiality Public	Page 1 of 1

SENQUIP VULNERABILITY DISCLOSURE POLICY

Revision	Date	Change
1.0	17 Sep 2026	First release

1. About this Policy

Senquip welcomes reports of security vulnerabilities affecting our devices, firmware, Senquip Portal, Senquip Connect and supporting services. This policy explains how to report a vulnerability and coordinate its disclosure.

2. Reporting a Vulnerability

Email support@senquip.com with the subject “Security vulnerability”. Include:

- Affected product or service, firmware or software version and relevant configuration;
- A description, potential impact and steps to reproduce the issue;
- Supporting evidence and a way to contact you.

Do not send passwords, private keys or customer data. If sensitive evidence is needed, contact us first to arrange a secure transfer. Report suspected active exploitation or immediate safety risks promptly.

3. How We Respond

We acknowledge reports promptly, assess their impact and investigate with our engineering team. We keep reporters informed of progress and coordinate with affected suppliers where necessary. Confirmed vulnerabilities are tracked to resolution, with remediation prioritised according to risk.

4. Coordinated Disclosure

Please report vulnerabilities privately and work with us on disclosure timing so protective measures can be made available. We discuss timing with the reporter, taking account of severity, active exploitation and risks to users. When fixes are available, we publish security information identifying affected products, the vulnerability and its impact, and recommended action. Disclosure may be delayed where necessary to protect users. Required notifications to users or authorities are not delayed by this coordination.

5. Responsible Testing

Test only devices, accounts and systems you own or are authorised to assess. Avoid disrupting services, changing live machine operation or accessing other people’s data. Stop testing and report the issue if you encounter sensitive information or a risk of harm. This policy does not authorise testing of Senquip’s live services or customer systems.