



VULNERABILITY DISCLOSURE POLICY

iLOQ Oy and its subsidiaries

Last Modified: 26th Nov 2025



Table of Contents

Contents

- 1. Purpose and Scope3
- 2. How to report a vulnerability3
- 3. Guidelines for researchers.....3
- 4. Recognition3
- 5. Document history3

1. Purpose and Scope

We are committed to ensuring the security and privacy of our products and services. We welcome reports of potential vulnerabilities from security researchers, partners, and customers.

2. How to report a vulnerability

If you believe you have discovered a security issue in one of our products, please contact us at: security@iloq.com

Please include:

- A clear description of the issue and affected product/version
- Steps to reproduce (if possible)
- Your contact information for follow-up communication

Our process

We acknowledge receipt of your report within 5 business days. We assess and verify the issue internally. We aim to provide updates on progress and coordinate disclosure responsibly.

If the issue is confirmed, we will address it through a security update or mitigation as soon as possible.

3. Guidelines for researchers

Do not publicly disclose the vulnerability before we have resolved it. Avoid accessing or modifying data that does not belong to you. Follow responsible disclosure practices at all times.

4. Recognition

We appreciate the contribution of all security researchers who help us keep our users safe. With your consent, we may acknowledge your responsible disclosure in our security advisory.

5. Document history

Version	Date	Author(s)	Comment
0.1	8.10.2025	H. Ahola	1st draft

0.2	8.10.2025	T. Ainali, J. Heusala, M. Hyvärinen, A. Timonen, H. Leskinen	Review
1.0	26.11.2025	Leadership Team	Reviewed and approved