AxonIQ

Responsible disclosure disclaimer

(exposed on the website AxonIQ)

AxonIQ B.V., Lange Viestraat 2b, 3511 BK, Utrecht	July 08,2025	vs 1.0 definitive

Principles

We consider the security of our systems a top priority. But no matter how much effort we put into system security, vulnerabilities can still exist.

If you discover a vulnerability, we would like to know about it to address it as quickly as possible. We ask you to help us better protect our clients and our systems.

Please do the following:

- E-mail your findings to security-disclosure@axoniq.io. Add the following information in the report:
  - A detailed description of the vulnerability.
  - Steps to reproduce the issue (if possible). Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.
  - Any relevant logs, screenshots, or other evidence that can assist our security team in understanding the problem.
  - You may also include a suggested mitigation or fix, but please note that we may not be able to follow these suggestions in all cases.
- Do not take advantage of or exploit the vulnerability or problem you have discovered, for example, by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data;
- Do not reveal the problem to others until it has been resolved;
- Do not use attacks on physical security, social engineering, distributed denial of service, spam, or applications of third parties
- Avoid Impacting Users, so do not perform any actions that could negatively impact other service users.
- Please provide sufficient information to reproduce the problem so we can resolve it as quickly as possible. Usually, the IP address or URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

What we promise:

- We will respond to your report within three business days with our evaluation of the report and an expected resolution date;
- We will handle your report with strict confidentiality and not pass on your personal details to third parties without your permission;
- We will keep you informed of the progress towards resolving the problem;
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise);

- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known. The reward amount will be determined based on the leak's severity and the report's quality. The minimum reward will be a €50 gift certificate.
- We strive to resolve all problems as quickly as possible and would like to play an active role in the ultimate publication of the problem after it is resolved.

Safe Harbor:

We believe responsible security researchers are invaluable in helping us improve our systems. If you follow this Responsible Disclosure Policy, we will not take legal action against you for discovering and reporting vulnerabilities in good faith.

Thank You:

We appreciate your efforts to help us keep our systems and users secure. Your contributions help us improve our security posture and ensure a safer experience for everyone.