# AXISNETWORKS - RESPONSIBLE DISCLOSURE

Date updated: 02/12/2025

AxisNetworks values the security of our infrastructure, services, and customers.

We appreciate responsible reporting of vulnerabilities and work hard to resolve issues quickly and transparently.

This Responsible Disclosure Policy outlines how security researchers and individuals may report vulnerabilities to AxisNetworks.

**1. INTRODUCTION**

Security is a top priority at AxisNetworks.

If you discover a security weakness or vulnerability within any of our systems, services, or applications, we ask that you report it responsibly and confidentially.

We do **not** pursue legal action against researchers who follow this policy in good faith.

This policy applies to:

- axisnetworks.org
- Customer portals & dashboards
- Network infrastructure, APIs, and backend systems
- Any subdomain or service owned and operated by AxisNetworks

**2. REPORTING A VULNERABILITY**

You can report vulnerabilities through:

noc@axisnetworks.org

Please include as much detail as possible, such as:

- Description of the vulnerability
- Steps to reproduce
- Potential impact
- IPs / URLs / endpoints affected
- Proof-of-concept (if applicable)
- Your contact information

Encrypted reports via PGP are available on request.

**3. WHAT YOU MAY TEST**

Testing is allowed on public-facing AxisNetworks systems **only if the tests do not cause service disruption**.

Permitted activities include:

- Local or remote testing for vulnerabilities
- Identifying authentication, authorization, or access control issues
- Detecting misconfigurations
- Examining publicly accessible endpoints
- Non-disruptive scanning with rate limits

**4. WHAT IS NOT ALLOWED**

The following actions are **strictly prohibited**, as they may cause harm:

- Launching DDoS attacks or stressing infrastructure
- Exploiting vulnerabilities to pivot deeper into systems
- Modifying or deleting data
- Accessing customer accounts or data
- Social engineering AxisNetworks personnel or customers
- Using automated brute-force tools
- Physical security testing without permission
- Testing must not degrade service performance, integrity, or availability.

**5. OUR COMMITMENT TO YOU**

If you follow this policy, AxisNetworks commits to:

- Acknowledging your report within **5 business days**
- Providing updates during investigation
- Resolving confirmed vulnerabilities as quickly as possible
- Never taking legal action against good-faith researchers
- Crediting you publicly (optional) on our **Security Hall of Fame**

We may offer rewards for high-impact findings, depending on severity and scope, but this is **not guaranteed** and not a formal bug bounty program.

**6. GOOD FAITH REQUIREMENTS**

To be considered a good-faith researcher:

- You must not compromise data availability, integrity, or confidentiality
- You must not access customer data or internal systems without authorization
- You must delete all data obtained through research immediately after reporting
- You must not publicly disclose the vulnerability before AxisNetworks resolves it
- You must follow coordinated disclosure timelines

Failure to follow these may result in investigation or legal action.

**7. SCOPE OF INFRASTRUCTURE**

Systems included under this policy:

- *.axisnetworks.org
- AxisNetworks APIs (cloud, network, cybersecurity)
- Customer portals and dashboards
- Network hardware (virtual testing only)

Out of scope:

- Third-party software not under AxisNetworks control
- Customer-owned equipment (e.g., colocated servers)
- Social media platforms

**8. RESPONSE PROCESS**

1. You submit the vulnerability to **noc@axisnetworks.org**
2. We acknowledge receipt
3. Our security team investigates
4. We classify severity (Low / Medium / High / Critical)

5. We schedule mitigation and patch deployment
6. We notify you upon resolution
7. (Optional) We publish a coordinated disclosure post

**9. LEGAL**

AxisNetworks will not take legal action against researchers who:

- act ethically and in good faith
- follow this Responsible Disclosure Policy
- do not exploit found vulnerabilities
- do not access or exfiltrate customer data
- do not publicly disclose before resolution

However, AxisNetworks reserves the right to investigate and take action against malicious actors or those who intentionally violate this policy.

**10. CONTACT INFORMATION**

For all responsible disclosure reports:

**AxisNetworks Network Operations Team**

Email: **noc@axisnetworks.org**
Website: **https://axisnetworks.org/**

PGP fingerprint available upon request.