Nozomi Networks Product Security and Information Security

At Nozomi Networks, we know you rely on our technology to protect some of the largest and most complex industrial environments in the world. To ensure that we will continue to earn your trust every day, you can count on us to:

- Develop, deliver and operate cybersecurity and visibility products for operational technology systems with the highest achievable level of quality, security, integrity and availability
- Protect corporate information, personal information, and customer data against loss, unauthorized access and disclosure

To deliver on our commitment to you, we rigorously follow industry best practices related to product security and information security.

Product Security

Within our software development life cycle and after release, we utilize several processes to identify potential product security issues:

- Adhere to the international standard ISO 9001:2015 for quality management and versioning conventions to ensure consistency, traceability and reproducibility
- Adopted best practices of secure software development, supporting the ISO 27001:2015 standard (see below)
- Conduct an internal vulnerability assessment on the continual build process
- Scan our entire code base regularly with automated tools to find potential vulnerabilities
- Monitor disclosures related to third-party software used in our operating system
- Ship our system image with a hardened and continually tested configuration
- Use third parties to scan our product for potential vulnerabilities after release
- Provide checksums of the compiled code for customer validation

After release, the **Nozomi Networks Product Security Incident Response Team** (PSIRT) is responsible for coordinating the investigation of any potential vulnerability in our products. If a security researcher discovers a potential vulnerability or security risk in one of our products, the PSIRT works with the engineering team to investigate the issue and identify any remediation when appropriate (our **Incident Response Policy** describes our approach in more detail). Nozomi Networks customers can **contact the Nozomi Networks PSIRT** directly using our **GPG key** to report any emerging vulnerabilities in their specific environments.

Remediation can be in the form of a software update and/or a temporary workaround. We tightly control information about any potential issue until remediation is available to avoid exposing our customers to security threats while a fix is still in development.

Once we make a solution available, we notify our customers about the issue and update the Security Portal.

Information Security

To secure all information assets, which includes all data we may collect from our customers, we use the Information Security Management System (ISMS) in support of the international standard ISO/IEC 27001:2015. To preserve the confidentiality, integrity and availability of our information, we have established and enforce a range of policies and procedures.

These policies and procedures include:

- General security requirements for the protection of information assets
- Restrictions on access and use of information assets
- Definition of roles and responsibilities for the protection of information assets

Nozomi Networks information protection policies include the following:

- Acceptable Use of Technology
- Access Control
- Data Handling
- Data Management and Retention
- Encryption
- Human Resources Security
- Information Asset Change Management
- Operations Security
- Password Security
- Personal Data
- Physical Security
- Security Incident Management
- System Configuration
- System Development and Maintenance
- Third Party Supplier Management

Use of Third Parties

At Nozomi Networks we are very aware of potential risks introduced with supply chain dependencies. We develop all of our software products in-house. In those cases where our products rely on third-party code to operate, we have customized our systems to minimize its use and the risk exposure. We assess all third-party products and providers associated with our business operations with a comprehensive due diligence program.

Our Employees

We carefully select, screen and evaluate our Nozomi Networks employees against the ethical standards of the company.

We seek and retain top cybersecurity talent from around the world to contribute to the development of our products and the security of our network infrastructure. They also deploy our product into our customers' networks, investigate incidents affecting our customers, and conduct research into the latest threats and trends. The combined result of these different teams' efforts is that we have developed additional proprietary and non-public methods of protection against cyber threats. These methods enhance the cybersecurity benefits derived from the product security and network security processes and policies described above.

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cybersecurity visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world. Our innovation and research make it possible to tackle escalating cyber risks through exceptional network visibility, threat detection and operational insight.

NN-PROD-SEC-8.5x11-001

nozominetworks.com