

Nihon Kohden

Product Security Framework



By ensuring cyber security throughout the entire *product life cycle* from development to post-sales support, we ensure that customers can always use Nihon Kohden products with peace of mind.

From Development to Production

Collecting and investigating vulnerability information

Security risks are detected by taking the software bill of materials (SBOM) that makes up the product, and collecting and investigating information on the vulnerabilities contained in each of those software components.

Design and implementation of security features

Security features are tailored to the specific characteristics of each product using a Secure-by-Design approach. In addition, software quality is maintained and improved through the use of tools such as static analysis tools.

Evaluation of security features

Security tests are tailored to the specific characteristics of each product to ensure that security features can be fully exploited in the environment in which the product is used by the customer.

Maintenance plan including EOL/EOS

Cybersecurity risk analysis

Internal systems and training to ensure compliance with laws and regulations

From Sales to Support

Monitoring and responding to vulnerability information

By continuing to monitor sources of vulnerability information, we can respond quickly to information on newly discovered vulnerabilities. In addition, we constantly receive information on vulnerabilities from both internal and external sources through the contact form on our website and respond appropriately to that information.

Provision of operator's manuals and customer security documents

In order to ensure that our products are used securely, the operator's manual for each product includes information on how to use the product's security-related functions as well as contact details for inquiries. In addition, a software bill of materials (SBOM) for the product and a disclosure statement on the security of the product or service will be provided upon request from the customer.

Disclosure of security advisories

Security advisories describing the impact of newly discovered vulnerabilities on Nihon Kohden products will be disclosed on our website as appropriate, taking into account the requirements of coordinated vulnerability disclosure (CVD) with ISAO/ISAC/CERT and other organizations and stakeholders.

Software updates

If we determine that our products are affected by newly discovered vulnerabilities, we will provide customers with updated software as appropriate.

Maintenance plans are prepared until the end of the product's life (EOL), and the end of support for the product (EOS). Also, customers are issued with warnings about continuing to use the product, and informed about additional security measures (e.g. installation of firewalls and offline operation disconnected from the network) that they can take.

Cybersecurity risk analysis is performed throughout the entire product lifecycle to reduce *risks leading to harm to the patient* and *risks related to information security* as much as possible.

To ensure compliance with product security laws and regulations, a PSIRT and other organizational structures have been established and internal training is provided to ensure that all employees are united in working to ensure product security.

- Explanation of Terms
- Cybersecurity: Maintaining risks related to the confidentiality, integrity and availability of information at an acceptable level over the entire lifecycle of a product.
 - Vulnerabilities: Flaws or weakness in the security of a system.
 - SBOM: Abbreviation of Software Bill of Materials. A list of software components used to build the product.
 - Secure-by-Design: A design philosophy that incorporates protections against unauthorized access and cyberattacks from the initial planning and design phases.
 - ISAO/ISAC/CERT: Organizations that share information on threats and vulnerabilities and conduct response activities.

- CVD: Abbreviation for Coordinated Vulnerability Disclosure. A process where vulnerability information is disclosed to the public after coordinating the contents and timing of the disclosure with the relevant stakeholders.
- EOL: Abbreviation for End of Life. The time when the life of a product ends.
- EOS: Abbreviation for End of Support. The time when support of a product ends.
- PSIRT: Abbreviation for Product Security Incident Response Team. A specialized team that responds to security incidents involving the company's own products and services.



Nihon Kohden has established and implemented the following product security policy

Product Security Policy

1. Compliance with Laws and Regulations

Nihon Kohden complies with all applicable laws and regulations of each country and region.

2. Structure

Nihon Kohden has established a product security structure and takes appropriate actions including providing necessary information and alerts to our customers and all other stakeholders.

3. Education

Nihon Kohden provides education and training on product security to all executive officers and employees throughout the Nihon Kohden Group in a timely manner, with the goal of increasing their awareness of product security.

4. Product Development

Nihon Kohden develops plans for ensuring security throughout the total product life cycle of each product. We also design and manufacture our products to minimize cybersecurity risk.

5. Post-market Response

Nihon Kohden collects information on security vulnerabilities affecting our products in a timely manner as well as implementing risk management and other appropriate measures to evaluate, eliminate, and control cybersecurity risk and other risks.

6. Information Sharing and Disclosure

Nihon Kohden shares security information required by our customers as appropriate.

To realize our Quality Policy:

“Maintaining high customer satisfaction with the purchase of a Nihon Kohden product through its entire life cycle,” Nihon Kohden has established and implemented this Product Security Policy to ensure cybersecurity throughout the total product life cycle from development to production, sales, and after-sales services.

The measures in this Security Policy by themselves are not sufficient to protect patients' and customers' information and financial assets from cybersecurity threats. A comprehensive and multi-layered security strategy that incorporates Nihon Kohden's contributions together with other security measures is required to protect patients' and customers' information and financial assets from cybersecurity threats.

Nihon Kohden asks our customers for their cooperation in ensuring product security.

NIHON KOHDEN CORPORATION

1-31-4 Nishiochiai, Shinjuku-ku, Tokyo 161-8560, Japan
Phone +81 3-5996-8041
<https://www.nihonkohden.com/>

Inquiries related to product security

<https://www.nihonkohden.com/contact.html>

