NIHON KOHDEN

Vulnerability Disclosure Policy

1. Objectives

Nihon Kohden is committed to ensuring cybersecurity over the full lifecycle of our products and services, so that patients, medical staff and customers can use them with peace of mind.
This policy covers the reporting and coordinated disclosure of undisclosed vulnerabilities in Nihon Kohden products and services.
The purpose of this policy is to support patient safety and continuity of healthcare by establishing a process under which the Company receives reports of vulnerabilities from security researchers, experts, users, and other external parties and works with the reporting parties and other stakeholders to carry out coordinated vulnerability disclosure.
Inquiries relating to product use, maintenance, quality, or other matters that do not constitute vulnerability reports are outside the scope of this policy. For all such inquiries, including urgent inquiries related to adverse events or patient safety, contact the appropriate department using the contact information relevant to your inquiry.

2. Reporting Vulnerabilities

Please report potential vulnerabilities using the following form:
Product security contact form: https://www.nihonkohden.com/contact.html#inquiry

To help us investigate the report and communicate efficiently with you, please supply the following information to the extent possible. Reports may be submitted even if not all of the requested information is available.

- Name, organization name and contact details of the reporter
- Name, model and version of the applicable product or service
- Details of the vulnerability, how it was discovered and steps required to reproduce it
- Potential impact, affected products and versions, extent of any known exploits
- Proof of concept code, logs and any other supporting information
- Status of notification of other vendors, regulatory authorities, coordinating bodies etc.
- Preferences related to disclosure
- Preferences regarding acknowledgement

We accept anonymous disclosures, but in that case we may be unable to confirm additional information and provide updates on the progress or results of the investigation. If the report contains sensitive information, provide only a summary in the initial report. We will contact you with instructions for securely providing additional information. Do not include the following information in your report: patient information, personal information belonging to third parties (other than the reporter), credentials, other confidential information unnecessary for the investigation. If you accidentally provide such information, notify us immediately.

3. Guidance for Responsible Vulnerability Testing

When performing testing, comply with all applicable laws and only test products for which you have obtained permission from the owner or rights holder. Conduct your testing with safety as your first priority and avoid any harmful impact on patients, medical staff and other hospital users.

The following activities are prohibited:

- Tests on any medical equipment while it is in use, in real clinical settings or on a live production system
- Conduct that would harm patients, interfere with care, or impair safety mechanisms
- Viewing, extracting, modifying or deleting data beyond the extent necessary to confirm a vulnerability
- Acquisition of patient information, personal information, credentials, and other confidential information
- Denial-of-service activities, actions that place excessive stress on systems, social engineering, or phishing
- Setting up backdoors, persistence mechanisms or other unauthorized functionality
- Unauthorized access to or testing of Nihon Kohden products and services, or those of third parties
- Publication of vulnerability details or reproduction information without prior coordination with Nihon Kohden

Once you have confirmed a vulnerability, conclude your investigation after performing only the minimum activities necessary to verify its impact, and report it in accordance with this policy.
This policy does not grant blanket permission to test Nihon Kohden’s or any third party’s products or services.

4. Nihon Kohden's Response

In principle, Nihon Kohden will confirm receipt within 5 business days of receiving a report. We will provide a reference number for issue tracking to reporters who have provided contact information.
After receiving a report we will proceed with the following actions based on the details and potential impact of the reported vulnerability:

- Verification of the contents of the report and investigation of the vulnerability
- Identification of the affected products and services
- Risk analysis based on patient safety, continuity of healthcare delivery, information security, exploitability, and the scope of affected products and users
- Contact other affected parties such as suppliers, regulatory authorities, and coordinating bodies

Our response period may vary depending on factors such as the impact of the vulnerability, the difficulty of remedying it, testing, regulatory procedures, and coordination across the product lifecycle and the supply chain. Nihon Kohden will establish an appropriate response strategy for each incident and will prioritize maximizing patient safety and minimizing risk to users. If there is any significant progress in the investigation or any major changes in our assessment, we will inform the reporter. When further time is

needed for the investigation or our response to it, we will, to the extent possible, explain the situation, the reasons and the planned next steps.

5. Coordinated Disclosure of Information

If you intend to publish vulnerability information, please contact us first. Nihon Kohden will, to give the highest priority to ensuring patient safety and minimizing the risk to customers, coordinate its response with affected parties including the reporter, regulatory agencies, national CERT [1]s , cybersecurity information-sharing organizations, and other vendors, and determine the timing and content of disclosure based upon the following points.

- Patient safety, continuity of healthcare delivery, known exploitation
- Availability of fixes, mitigation strategies, and workarounds
- Notification of users, regulatory requirements, status of coordination with third parties

When additional time is required before disclosure, we will, to the extent possible, explain the situation and the reasons for the delay to the reporter. We will publish a summary of the vulnerability and its tracking identifier, the affected products and versions, the impact and severity, any fixes, mitigation measures, workarounds, and other relevant information in security advisories, as appropriate. However, information that could adversely affect safety or the rights of any party may be omitted or appropriately redacted.

6. Response to Reporters and Handling of Information

We will investigate and address vulnerabilities reported in good faith in accordance with this policy, while cooperating sincerely with the reporter. We will not take adverse action against a reporter solely because they reported a vulnerability to us, provided the investigation and reporting were conducted with permission and in accordance with this policy, and in a way that had no adverse impact on patients or medical institutions.

However, compliance with this policy does not guarantee compliance with applicable laws or regulations, or exemption from liability, nor does it authorize any action for which we have not given explicit permission. Nor do we make any guarantee for the decisions and responses of third parties in relation to their systems and services.

We will only handle vulnerability information to the extent necessary for investigation, response, and coordination with relevant parties. Access to unpublished vulnerability information is limited to personnel involved in handling the case and only to the extent necessary to perform their roles. The reporter’s personal information will be handled according to Nihon Kohden's Personal Information Protection Policy.

When requested by the reporter and deemed appropriate by Nihon Kohden, an acknowledgement of the reporter may be included in a security advisory with the reporter's consent.

Requests for anonymous publication, publication under a pseudonym, or omission from the acknowledgements will also be accommodated. This policy is not a bug bounty program and no financial or other reward will be paid for vulnerability reports.

---

[1] CERT: Computer Emergency Response Team.

7. Other

This policy is not a substitute for activities and procedures related to product safety, quality, legal and regulatory reporting obligations, or other required processes.
We will revise this policy in response to changes in laws, regulations, technology, and operational requirements, and publish the revised policy on our website.

Issue Date:2026-10-01
Version:1.0