Coordinated Vulnerability Disclosure Policy

1. Purpose

RIKEN KEIKI Co., Ltd. (“the Company”) establishes this Policy to define the process for receiving vulnerability reports and disclosing related information. The purpose of this Policy is to help maintain and improve the safety, reliability, and quality of the Company’s products by enhancing product security and reducing cybersecurity risks that could affect people, equipment, or business continuity.

2. Reporting Vulnerabilities

The Company accepts vulnerability reports concerning its products through the Product Vulnerability Inquiries contact form below.

This contact form is intended solely for product vulnerability reports and related inquiries. For security incidents affecting the Company’s information systems, product defects, or general inquiries, please use the appropriate contact point for the relevant type of inquiry.

In Scope

- Products provided by the Company that fall within the scope of the Cyber Resilience Act (CRA)

Out of Scope

- Products for which security support has ended
- Evaluation products and products being used on a trial basis
- Vulnerabilities arising from third-party products or services that the Company does not manage or maintain

Reports based on testing involving excessive system loads, DoS or DDoS attacks, data destruction or alteration, or physical attacks may not be handled under this Policy.

Product Vulnerability Inquiries

https://www.rikenkeiki.co.jp/english/contact/products_psirt

Vulnerability Information

https://product.rikenkeiki.co.jp/english/news/product-security/

Note: For products manufactured by a third party, please contact the relevant manufacturer.

Note: Information submitted through the contact form is encrypted in transit using HTTPS. If confidential information must be exchanged by email, the Company may use encryption features available in Microsoft Outlook or another appropriate secure communication method. Where necessary, the Company will coordinate with the reporter to determine an appropriate method for securely exchanging information.

3. Guidelines for Reporters

Please follow these guidelines when reporting a vulnerability:

- Limit testing to the minimum extent necessary to confirm the vulnerability and avoid any unnecessary impact.
- Do not access or obtain personal or confidential information beyond what is necessary to confirm the vulnerability. Do not alter or destroy data or conduct DoS or DDoS testing.
- If you intend to disclose vulnerability information to any third party, please coordinate the timing of disclosure with the Company in advance.

4. Information to Include in a Vulnerability Report

To facilitate the prompt investigation of and response to a vulnerability, the Company may ask you to provide the following information, where available:

- Reporter's name and contact details
- Name and model number of each affected product
- Description of the vulnerability and any observed behavior
- Steps to reproduce the vulnerability
- Potential or observed impact
- Information on any available workarounds or mitigation measures
- Any related identifiers or references, such as CVE identifiers
- Applicable software and firmware versions

If the vulnerability affects products from multiple vendors, please indicate, where possible, whether it has also been reported to other affected vendors.

5. Acknowledgment and Initial Response

When the Company receives a vulnerability report through the Product Vulnerability Inquiries contact form, it will promptly acknowledge receipt.

The Company may request additional information as necessary to review and assess the report.

Where appropriate, the Company will keep the reporter informed of the progress of its investigation and remediation efforts.

6. Handling and Disclosure of Vulnerability Information

Until remediation is complete and the vulnerability information is publicly disclosed, the Company will limit access to such information to those who need to know and will minimize the risks associated with premature disclosure.In principle, the Company will prioritize user safety and disclose vulnerability information after a fix or effective workaround becomes available.

Information will be handled in accordance with applicable laws and regulations and any applicable non-disclosure agreements (NDAs).

The Company will publish vulnerability information on its website or through another appropriate channel.

Published information will include the information necessary for users to take appropriate action, such as the affected products and versions, the impact and severity of the vulnerability, and available remediation measures, including update instructions and workarounds.

If the Company determines that the risks of disclosure outweigh its benefits, the Company may adjust the timing of disclosure after allowing users a reasonable period to apply a fix or implement an effective workaround.

7. Safe Harbor for Good-Faith Reporting

If a reporter complies with this Policy, reports a vulnerability in good faith and in a cooperative manner, and conducts any verification activities in accordance with this Policy, the Company will generally refrain from initiating or pursuing legal action against the reporter for those activities. The Company will also not subject the reporter to unfavorable treatment solely because the reporter submitted the report in good faith.

This safe harbor does not apply to activities that violate applicable laws or regulations or infringe the rights of any third party.

8. Recognition of Reporters

The Company appreciates the cooperation of individuals who report vulnerabilities in good faith and values their contributions.

At the reporter’s request, the Company may publicly acknowledge the reporter by name or handle when publishing information about the vulnerability.

The Company does not currently maintain a vulnerability reward or bug bounty program.