Vulnerability Disclosure Policy

To ensure product security and safe use of our products by customers, we have established a PSIRT (Product Security Incident Response Team). The PSIRT is committed to identifying, assessing, and handling product vulnerabilities. In compliance with ISO/IEC 29147 standards and Information Security Early Warning Partnership Guidelines, we will disclose vulnerability information in a timely and appropriate manner, and work cooperatively with the reporters to provide appropriate vulnerability management and help reduce customer security risks.

1 Basic Policy

We regard the safety and reliability of our products and related services as highly important, and endeavor to ensure cybersecurity through the entire product lifecycle.
Based on the premise that vulnerability is unavoidable, we have established a system for appropriately identifying, reporting, and resolving vulnerabilities.

2 Scope

This policy applies to the products we develop, manufacture and provide, as well as the software, firmware and cloud services associated with them.

3 Reporting a Vulnerability

If you discover a security vulnerability in any of our products, report it to us via the link below.

Click here to report a vulnerability.

Where possible, please provide us with the following information:

- Name and version of the affected product
- Description of the issue and how to reproduce it
- Possible impacts

4 How We Respond to Vulnerability Reports

Upon receiving a report, we will review the reported vulnerability and assess severity and urgency. We will then provide corrective measures, workarounds, or information as needed.

5 Cooperative Vulnerability Disclosure

We welcome vulnerability reports based on good intentions and will not take any legal action against the reporters. We expect your cooperation in the disclosure of vulnerability information until the issue has been resolved.

6 Personal Information Handling

We only use personal information obtained from your reports for the purposes of handling vulnerability issues.

This policy is subject to change without prior notice.

DAIHEN