Product Security Policy

1. Basic Policy

We recognize cybersecurity as an essential component of the quality of our products and services.
We are committed to ensuring appropriate product security throughout the entire product lifecycle, including planning, design, development, delivery, and maintenance.

We strive to reduce cybersecurity risks that may compromise the confidentiality, integrity, and availability of our products, and to maintain an environment in which customers can use our products safely and securely.

2. Compliance with Laws and Standards

We comply with applicable laws, regulations, and industry standards related to product security in the countries and regions where we operate.

In addition, we continuously improve our practices by referring to internationally recognized frameworks and standards, including:

ISO/IEC 29147 (Vulnerability Disclosure)
ISO/IEC 30111 (Vulnerability Handling)

We also monitor developments in cybersecurity regulations for products, including the EU Cyber Resilience Act (CRA), and are working to establish the necessary organizational structures and operational processes.

3. Product Development and Quality Initiatives

We incorporate cybersecurity considerations from the early stages of product design and development.

Identifying and assessing risks during the design phase
Applying appropriate design, implementation, and verification processes
Implementing measures that take into account product usage and operating environments

Through these efforts, we aim to minimize security risks associated with our products.

4. Response to Vulnerabilities and Incidents

When we become aware of vulnerabilities or security issues in our products, we take appropriate evaluation and corrective actions.

Verification and impact assessment of reported vulnerabilities
Development and implementation of remediation or mitigation measures
Information sharing and disclosure as necessary

In particular, when there is a potential impact on the safe use of products, we strive to provide users with sufficient information to enable appropriate decisions and responses.

5. Vulnerability Handling and Disclosure

We recognize responsible vulnerability reports from external parties as an important source of information and provide appropriate channels to receive such reports.

We may disclose information related to vulnerability handling at an appropriate extent and timing, in coordination with relevant stakeholders, based on the principles of coordinated vulnerability disclosure and initiatives such as Early Warning Partnerships, with the aim of ensuring product safety and protecting users.

We strive to provide clear and understandable information regarding the availability of fixes and the actions users should take.

6. Continuous Improvement

We regularly review and improve our product security framework and initiatives in response to evolving threats and technological advancements.

Through these efforts, we aim to enhance product reliability and contribute to the safety and peace of mind of our customers.