SEG
an Arteche Company

Vulnerability disclosure policy

September 2026

01

Vulnerability disclosure policy

In SEG, the security of our products is a priority. We are aware that when vulnerabilities are detected and exploited, the confidentiality, integrity or availability of the systems and/or applications in which Arteche products are installed can be jeopardized.

This Vulnerability Disclosure Policy describes what systems and types of testing are authorized. We encourage you to disclose information security issues responsibly and in accordance with this Vulnerability Disclosure Policy.

02

Authorization

Researchers and security professionals should feel comfortable reporting discovered vulnerabilities to us as defined in this policy. As long as this process is used correctly when disclosing security issues to Arteche Group, we will not take legal action or revoke your access to our products and/or applications.

SEG reserves all legal rights in case of non-compliance.

03

Scope of application

This policy applies to those products that use Arteche Group‘s digital elements:

- Control equipment
- Protective equipment
- Measuring equipment
- Sensor equipment

Services not mentioned are excluded from the scope of application and cannot be tested without our express authorization. Vulnerabilities detected in third-party devices are also excluded and should be reported directly to the vendor or manufacturer in accordance with their own disclosure policy.

04

Guidelines

4.1. Obligations when conducting your research or testing

- Do not illegally access systems in production. If the access is accidental or public, you must notify the person in charge of the infrastructure where the equipment is installed, or csirt@segelectronics.de, or the CSIRT of reference.
- Do not exploit the vulnerability or problem you have discovered. For example, downloading more data than necessary to demonstrate the vulnerability, deleting or modifying the data.
- Use only harmless applications / tools / payloads, only if necessary, to confirm the existence of a vulnerability.
- Do not disclose any data downloaded during discovery to the public or to any other party.
- If you find sensitive information, such as personal identifiable information, financial or confidential information, or trade secrets, stop testing immediately, notify us and do not disclose any data obtained to anyone else.

4.2. Prohibited actions

- Introduce malware (viruses, worms, Trojans, etc.) into a product and/or infect personnel involved in the life cycle of any product.
- Putting a system at risk by means of intrusive programs to obtain total or partial control.
- Copy, modify or delete product data
- Introducing product changes
- Repeatedly accessing the product or sharing access with the public or other parties
- Using any access gained to attempt to access other systems
- Change access rights of other users
- Using brute force or dictionary techniques to access any product
- Employing denial of service techniques
- Use of social engineering techniques (phishing, vishing, spam, etc.)
- Using physical security attacks

4.3. Legal

As part of the Arteche Group, SEG Electronics GmbH applies the Arteche legal framework for vulnerability disclosure. The following legal requirements are adopted without any changes.

This policy is designed to be consistent with standard good practice in vulnerability disclosure. It does not give you permission to act in any way that is inconsistent with the law, or that may cause Arteche to breach any of its legal obligations.

Applicable Laws and Regulatory Requirements:

- the General Data Protection Regulation (GDPR) (EU) 2016/679;
- the Cyber Resilience Act Regulation (CRA) (EU) 2024/2847;
- applicable national data protection laws;
- laws relating to intellectual property rights and copyright;
- laws relating to the protection of trade secrets and confidential business information;
- applicable cybersecurity, computer misuse, and unauthorized access laws;
- any other applicable regulatory requirements relevant to SEG products and their deployment environment.