Franke is committed to ensuring the security of its websites, connected products and mobile applications that interact with online services. This policy provides guidelines for anyone who conducts vulnerability discovery and identifies any vulnerabilities, and a process for reporting such vulnerabilities to Franke.

We recommend reading this vulnerability disclosure policy fully before you report a vulnerability. We value those who take the time and effort to report security vulnerabilities according to this policy.

Franke is keen to reward reports addressing significant vulnerabilities with a bounty payment up to 2'000 CHF. Whether a reward is awarded remains always at Franke's discretion; the amount paid, if any, also remains at Franke's discretion. In no event shall there be a legal entitlement to a reward. Qualifying reports need, at a minimum, to fulfill following requirements:

- Design or implementation issues that pose a significant risk potentially allowing attackers to cause substantial damage or gain complete control over the affected system, typically CVSS 8.0 or higher.
- Proof of Concept is provided to Franke security, and Franke security can recreate the exploit independently on live systems.
- The vulnerability is not previously known by Franke security.
- The reporter is not affiliated with Franke or its partners
- The reporter is on sanctioned lists or in countries on sanctions lists.
- The product has to be designed and maintained by Franke; products recently acquired may be ineligible. For impacted third party products we will provide the correct point of contact.

**Reporting a Vulnerability:**
If you believe you have found a security vulnerability related to Franke, please submit your report to us using the following email: security@franke.com

In your report, please include details of:
**1 - Affected product:**

- product type (app or appliance)
- product model and version

**2 - Description of the Vulnerability:**

- a summary of the vulnerability
- add any helpful supporting files (e.g., screenshot or video) if available
- add any mitigations or recommendations

**3 - Steps to reproduce:**

- Clear and descriptive steps to reproduce the vulnerability.
- estimated impact of the vulnerability
- proof of concept code, exploit code, network traces, other resources demonstrating the vulnerability or how-to exploit the vulnerability.

Note: If a large amount of data needs to be submitted, please contact us, and we will arrange the proper way to exchange information

**4 - Public references (if any):**

- Please indicate if the vulnerability has already been publicly disclosed and by whom (provide us the reference).

**Guidelines to follow:**
To participate in Franke's vulnerability disclosure program, participants must:

- Submit reports in English. (We will discard non-English communication.)
- Comply with all applicable laws.
- Adhere to this policy and other applicable agreements.
- Allow Franke a reasonable amount of time to analyze and/or resolve the issue before publicly disclosing it.
- Not access or modify Franke's or users' data without explicit permission from the owner and immediately contact Franke if accidental user data access occurs.
- Avoid privacy violations, placing backdoors, data destruction, and disruption or degradation of our services (including denial-of-service attacks). Avoid the use of high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Do not attempt to manipulate Franke employees or contractors for access or information.
- Focus on verifiable vulnerabilities that pose a risk. General configuration issues like TLS cyphers, email spam, volumetric attacks, missing web security headers, reports from automated web vulnerability scanners without manual verification or "best practices" alone are not considered unless they are part of an exploitable condition.
- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

**What to expect from our revision process:**
When Franke receives a vulnerability report, we acknowledge its receipt within 10 business days and provide an estimated timeline for resolution. Franke aims to fix all valid vulnerabilities within 90 working days of reporting, although more time may be needed for complicated fixes.

We will also aim to keep you informed of our progress. Priority for remediation is assessed by looking at the impact, severity, and exploit complexity. We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately. We will publish a security advisory or technical note to inform users and the community.

Remember that reporting can be done anonymously. We do not need any personal data of the reporter except basic information to pay the bounty when applicable.

**Additional considerations:**
We strongly recommend PGP encryption in your initial email communication.
This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause the Organization or partner organizations to be in breach of any legal obligations.