COORDINATED VULNERABILITY DISCLOSURE POLICY

in Execution of the Regulatory Requirements of the
Cyber Resilience Act (CRA) of the European Union

Preamble

In fulfillment of the regulatory obligations as well as the statutory duties of care in accordance with the provisions of the European Cyber Resilience Act (CRA), this policy constitutes the formal framework for the orderly handling of security-relevant anomalies. It standardizes the binding procedure for reporting, evaluating, and remediating potential vulnerabilities, with the primary protective purpose of maintaining the integration and data security of the user base.

§ 1 Material and Territorial Scope of Application

The dispositions of this policy shall have full and unconditional legal effect for any and all software-based as well as software-defined products. This subsumes all pure software applications as well as hardware-bound systems (T+A products), provided that they possess integrated firmware or software components and are developed or placed on the market under the administrative or copyright responsibility of our company.

§ 2 Formal and Time-Bound Submission of Vulnerability Reports

Subjects, whether natural or legal persons (hereinafter: Reporter), who obtain knowledge of a security-relevant vulnerability in the products defined under § 1, are obliged in the interest of damage prevention to report this immediately. In order to satisfy the formal requirements for secure and legally robust documentation, the submission of the report must strictly and exclusively occur via the telemedia reporting form (e-mail form) implemented on the official website. Alternative methods of transmission do not initiate any statutory periods and shall be deemed as not formally submitted.

§ 3 Material Requirements for the Vulnerability Report (Duty of Substantiation)

To ensure an appropriate, reproducible, and procedurally economical verification of the reported facts, the transmission of specified technical parameters is required. Taking into account the dynamics of asymmetrical threat scenarios, a static enumeration of the required data sets is omitted in this document. Instead, binding reference is made to the information matrix provided at the URL **ta-hifi.de/cra**. The specifications maintained there on a daily and needs-adjusted basis are hereby deemed an integral part (per relationem) of this policy.

§ 4 Internal Evaluation and Mitigation Procedure

The formally correct receipt of any report initiates a predefined, multi-stage review procedure:

- **Classification and Triage:** Initial formal and material plausibility check to determine the validity of the report.
- **Interdisciplinary Fact-Finding:** In-depth forensic and systemic analysis by authorized expert committees. The mandatory participation of the relevant departments, namely development, production, and manufacturing, is strictly required herein.
- **Remediation:** Upon positive verification of the vulnerability, measures for damage prevention (mitigation, patch provision, or firmware update) shall be initiated immediately.

§ 5 Information Exchange and Data Protection Provisions

The bilateral interaction with the Reporter is subject to strict behavioral and confidentiality stipulations:

- **Data Protection Compliance:** The processing of any personal data of the Reporter shall be carried out in strict compliance with Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR).
- **Principle of Necessity:** Any follow-up inquiries by the security team for the purpose of fact-finding or reproducibility shall be made in observance of the principles of proportionality and adequacy of need via secure and appropriate communication channels.

§ 6 Publicity Restrictions (Coordinated Vulnerability Disclosure)

The indispensable principle of coordinated and sanctioned disclosure shall apply. The Reporter is subject to a comprehensive duty of confidentiality (Non-Disclosure). The Reporter is prohibited from communicating details regarding the identified vulnerability in whole or in part to third parties or the public without explicit written authorization. A publication may occur at the earliest at the point in time when the internal analysis and remediation process is fully concluded and appropriate protective mechanisms (security updates) are available to the affected end users.

§ 7 Temporal Deadlines and Modalities of Feedback

Subject to any mandatory statutory provisions to the contrary, the following temporal dispositions shall apply to ensure compliance with the EU CRA:

- **Deadline for Initial Response:** The formal confirmation of receipt of the report (initial response) shall be issued within a maximum time frame of 30 hours from the receipt of the report, calculated exclusively in business days based on Central European Time (CET).
- **Intervention and Reporting Duties:** The further investigation of the vulnerability as well as the fulfillment of any reporting obligations to state or supranational supervisory authorities shall be carried out strictly in accordance with the statutory deadlines of the EU CRA.

- **Substantiated Feedback (Feedback Loop):** Depending on the prospective damage class and the systemic classification of the vulnerability, the Reporter shall be provided with a substantiated statement regarding the further procedural course of action no later than 6 weeks after the confirmation of receipt.