Central Coordinated Vulnerability Disclosure Policy

Version 1.0.1

Author	TTTECH CISO
Owner	Information Security Governance Team
Applicability	See Applicability Section
First Release Date	10/09/2026
Classification	PUBLIC
Status	Released
Document ID	D-000-POL-04-017

Version Control

Version	Date	Name	Change
1.0.1	10/09/2026	TTTECH CISO	Minor role clarification Link update

Reviewers and Approvers

Name	Title	Role
Intentionally Empty	Security Representative of TTControl (Brixen)	Reviewer
Intentionally Empty	Security Representative of TTControl (Vienna)	Reviewer
Intentionally Empty	Security Representative of TTTECH Aerospace	Reviewer
Intentionally Empty	Security Representative of TTTECH Computertechnik	Author
Intentionally Empty	Security Representative of TTTECH Digital	Reviewer
Intentionally Empty	Security Representative of TTTECH Industrial	Reviewer
Intentionally Empty	Security Representative of TTTECH Japan	Reviewer
Intentionally Empty	Security Representative of TTTECH North America	Reviewer
Intentionally Empty	Change Control Board	Approver (approvals documented in Artifact Records).

Short Description

TTTECH recognises that responsible security research and timely vulnerability reporting contribute significantly to improving cybersecurity and protecting customers, users, and business operations.

Therefore, the primary purpose of this Coordinated Vulnerability Disclosure (CVD) Policy is to provide a clear, transparent, and structured process for the reporting, assessment, remediation, coordination, and disclosure of security vulnerabilities affecting TTTECH products, services, and systems.

Scope

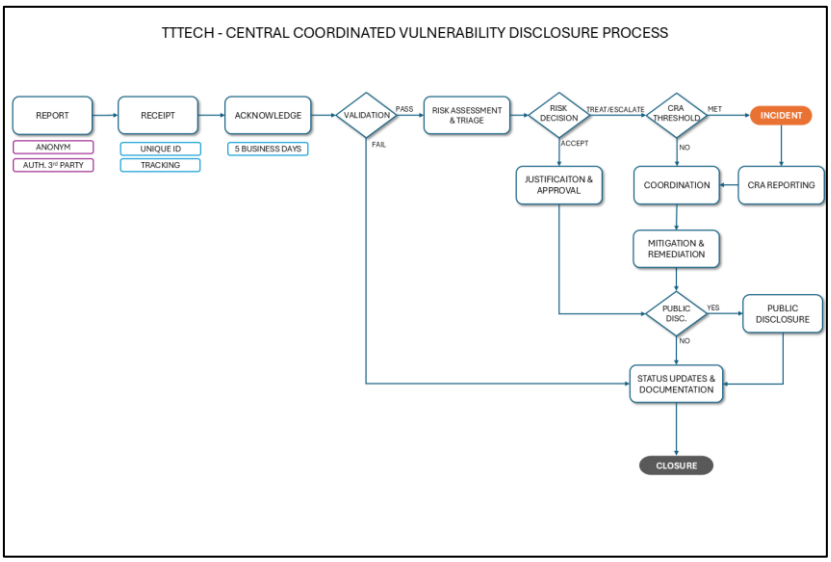
While local operational responsibilities and applicable legal requirements are maintained, a common vulnerability disclosure framework is followed across all TTTECH business entities, products and services, including:

- TTControl (Brixen)
- TTControl (Vienna)
- TTTECH Aerospace
- TTTECH Computertechnik
- TTTECH Digital
- TTTECH Industrial
- TTTECH Japan
- TTTECH North America

Applicability

Security researchers, customers, suppliers, employees, government authorities, CERTs, CSIRTs, trusted disclosure coordinators, and any other internal or external party acting in good faith.

Graphical Process View



1. Vulnerability Reporting Channels

1.1 Anonym Reporting Channel

The main, publicly accessible vulnerability reporting contact and mechanism is through the Responsible Disclosure form via the main TTTECH website:

- Responsible Disclosure - TTTECH
- Responsible Disclosure - TTControl

Reporters may choose not to provide identifying information in the form, however, anonymous reports may limit TTTECH's ability to request clarification, reproduce findings or provide feedback regarding the status of the report.

1.2 Authenticated Reporting Channel

Authenticated reporting channels for customers, suppliers, and other authorised stakeholders are possible via the dedicated TTTECH customer ticketing service.

2. Expectations for Security Researchers and Reporters

Vulnerabilities shall be reported through one of the previously detailed reporting channels.

Reports shall contain sufficient information to allow verification and assessment of the reported issue, including affected products, affected versions, technical details, proof of concept where available, and contact information if follow-up communication is desired.

During security research and testing, reporters/researchers shall:

- avoid service disruption,
- avoid unauthorized access beyond what is necessary to demonstrate the vulnerability,
- avoid modification, deletion, disclosure, or retention of data,
- avoid actions that could affect safety-related functions, and
- comply with applicable laws and regulations at all times.

3. Good Faith Reporting and Safe Harbor

Reports submitted in good faith and in accordance with this policy will be reviewed and handled through the coordinated vulnerability disclosure process.

Good faith reporting includes:

- reporting a genuine security concern,
- using reasonable efforts to avoid harm,
- cooperating with requests for clarification, and
- maintaining confidentiality during the disclosure process.

The following activities are not regarded good faith and may be referred for legal or regulatory action:

- extortion or coercion,
- data theft,
- malware deployment, and
- any other malicious and unlawful activity.

The determination of good faith remains at the reasonable discretion of TTTECH.

4. Vulnerability Handling Process

4.1 Receipt

All valid reports are logged and assigned a unique identifier.

4.2 Acknowledgement

Receipt of a vulnerability report is acknowledged within a maximum of 5 business days.

Where contact information is available, a communication channel is established with the reporter.

4.3 Validation

Reported vulnerabilities are reviewed to determine whether:

- the issue is reproducible,
- the issue affects a product, service, or system within scope,
- sufficient information has been provided, and
- the reported issue represents a security vulnerability.

Invalid, duplicate, or out-of-scope reports may be closed.

Anonymous reports may limit TTTECH's ability to request clarification, reproduce findings or provide feedback regarding the status of the report.

4.4 Risk Assessment and Initial Triage

Validated reports are scored and prioritised using the Common Vulnerability Scoring System (CVSS) or the applicable cybersecurity vulnerability management procedures, considering at minimum the:

- severity,
- exploitability,
- exposure,
- active exploitation status,
- safety impact,
- customer impact, and
- regulatory obligations.

If a vulnerability meets reporting thresholds under applicable law or contractual requirements, TTTECH will promptly notify the relevant competent authorities and customers.

When a vulnerability is closed through risk acceptance, the closure record shall document the justification, identified risks, compensating controls, and approving authority.

4.5 Coordination

TTTECH may coordinate remediation activities with:

- Product cybersecurity teams,
- Suppliers and customers,

- CERTs and CSIRTs,
- ENISA, and
- Other third parties, including public authorities.

Where appropriate, such organizations may be used as trusted intermediaries to facilitate coordinated disclosure or manage complex multi-party cases.

4.6 Mitigation and Remediation Timeline

Following the initial triage, mitigating and remediation measures are developed by the appropriate product cybersecurity and developer teams.

Such activities aim to follow the Baseline Remediation Timelines (Table 1), however, other remediation targets may be applicable depending on the affected product, business entity, customer deployment constraints, safety impacts, supplier dependencies, and contractual/legal requirements.

Severity	**CVSS Score**	**Target**
Critical	≥ 9.0	7 days
High	7.0 – 8.9	14 days
Medium	4.0 – 6.9	2 months
Low	0.1 – 3.9	4 months
Actively exploited vulnerability or significant security impact	Escalated immediately as a security incident to the central security functions.	

Table 1 - Baseline Remediation Timelines

4.7 Coordinated Public Disclosure

TTTECH will not publicly disclose details of vulnerabilities until mitigating measures or security updates have been developed and made available to customers, or where publication would create a higher security risk or increase the likelihood of exploitation.

We ask researchers and reporters to adhere to this approach as well and coordinate any independent publications with us prior to release.

In case a decision to disclose is made, TTTECH security advisories describe at minimum:

- the vulnerability,
- affected products,
- severity,
- potential impact,
- actionable remediation guidance,
- credits to the reporter, when desired and appropriate.

4.8 CRA Reporting

According to the Cyber Resilience Act, the following reporting thresholds are observed by TTTECH:

1. Actively exploited vulnerabilities affecting a product with digital elements, and
2. Severe incidents affecting the security of a product with digital elements.

Regulatory reporting is done through ENISA Singe Reporting Platform (SRP) following the below reporting timelines:

Report Type	**Deadline**	**Minimum Information**
Early Warning	Within 24 hours	Initial indication that an actively exploited vulnerability or severe incident has been identified
Notification	Within 72 hours	Initial assessment, affected products, exploitation details (if known), mitigation measures, and current status
Final Report	Within 14 days after a corrective measure becomes available (actively exploited vulnerabilities)	Complete technical information, root cause, impact assessment, remediation details, and lessons learned
Final Report (Severe Incident)	Within 1 month after the 72-hour notification	Final incident analysis and corrective actions taken

4.9 Customer Reporting

In cases where legal or contractual obligations mandate notifications to customers, the relevant product owner takes the required steps to ensure that these are actioned accordingly.

4.10 General External Vulnerability Reports

Vulnerability reports to customers and authorities include all information reasonably known at the time and updated through subsequent reports as additional details become available. At a minimum, reports include:

- manufacturer name and contact details,
- reporting contact person,
- product name, version, and affected releases,
- description of the vulnerability or incident,
- date and time of awareness,
- current exploitation status,
- known indicators of compromise,
- preliminary assessment of impact,
- customer impact assessment,
- known mitigations,
- planned remediation measures, and
- expected timeline for corrective actions.

5. Closure

Vulnerability reports are closed only after all applicable activities have been completed, including:

- the vulnerability assessment has been documented,
- required remediation or mitigation activities have been completed,
- required contractual / regulatory reporting obligations have been fulfilled,
- any required security advisory has been published, and
- the reporter has been informed of the final disposition of the report.