Coordinated Vulnerability Disclosure Policy

Document No.	CRA-CVD-001
Version	V1.0
Date of issue	2026-09-03
Prepared by	Jin Cancan
Reviewed by	Zhou Yang
Approved by	Zhou Yang
Product	Nand Flash Tracer (NFT)
Language	English (Official Version for EU Market Surveillance Authorities)

1 Purpose and legal basis

This policy publishes to security researchers, users and other interested parties the single point of contact for reporting vulnerabilities in the manufacturer's product and the rules for intake and coordinated disclosure, so as to satisfy the requirements of Annex I Part II, points (5) and (6), Article 13(17) and Annex II, point 2 of the CRA concerning the single point of contact and the coordinated vulnerability disclosure policy.

Reference: Regulation (EU) 2024/2847, Annex I Part II, points (5) and (6); Article 13(17); Annex II, point 2.

2 Scope

This policy applies to any vulnerability, discovered internally or externally, that affects the essential cybersecurity requirements of the NFT software (assessed baseline version Ver 2.26.8 and later versions released during the support period).

3 Single point of contact (reporting intake)

The manufacturer designates the following single point of contact for receiving vulnerability reports and for consulting this coordinated vulnerability disclosure policy:

- Vulnerability reporting email: nandflashtracer@gmail.com (currently published address)

> A dedicated vulnerability reporting inbox security@flash-tracer.com is established and pinned on the website and forum.

- Policy consultation address: https://www.flash-tracer.com/ (compliance page, https://www.flash-tracer.com/about.html) and https://www.flash-tracer.com/bbs/forum.php

Reference: Article 13(17). The single point of contact shall be easily identifiable, included in the user information and instructions (Annex II, point 2), and shall allow users to choose their preferred means of communication; it shall **not be limited to automated tools**. Therefore, besides email, the manufacturer also accepts contact via the website forum private message and by telephone at +86 15524692190.

4 Intake and acknowledgement

- Upon receipt, the Vulnerability Coordinator shall acknowledge within **3 working days** and provide the reporter with an intake reference (consistent with the log in the Vulnerability Handling Process, CRA-VHP-001).
- The manufacturer does not discriminate by reporting channel (email, forum, telephone) and does not reject a report on the basis of the reporter's identity.
- Reporters may choose their preferred language and channel of communication within feasible limits.

5 Coordination principles

- The manufacturer assesses and rates the report under the Vulnerability Handling Process (CRA-VHP-001) and maintains necessary communication with the reporter.
- Within reasonable limits, the manufacturer coordinates with the reporter on the timing of remediation and public disclosure, avoiding unilateral premature or delayed disclosure.
- Sensitive materials provided by the reporter (PoC, logs, etc.) are used solely for remediation and are not forwarded without authorisation.

6 Disclosure timing

- Coordinated disclosure by default: from intake, the manufacturer is given a reasonable remediation window (generally not less than 90 days, negotiated according to severity); the vulnerability information is publicly disclosed after the security update is released (Annex I Part II, point (4)).
- Where there is justified reason to consider that the public security risk outweighs the security benefit, disclosure of the remediated vulnerability may be delayed until users have had the opportunity to apply the patch (the proviso to Part II, point (4)).
- For an actively exploited vulnerability or significant incident, the Vulnerability and Incident Reporting Procedure (CRA-IRP-001) takes priority under Article 14 deadlines, and affected users are informed in parallel.

7 Reporter rights and safe harbour

- The manufacturer thanks reporters and may, with the reporter's consent, give public acknowledgement. No bug bounty programme is currently established; if one is introduced in future it will be announced separately.
- Good-faith reporting conducted in accordance with this policy will not be subject to legal action by the manufacturer. Reporters must comply with applicable law and must not perform denial-of-service attacks, access unauthorised data, or affect third-party systems.

8 Policy maintenance

- This policy remains effective throughout the support period and is accessible on the website compliance page and in the user information and instructions, kept online for at least 10 years or the support period, whichever is longer (Annex II and Article 13(18)).
- Changes are reflected in the version and date and announced via the website and forum.

9 Items pending confirmation

1. Establishment and publication of a dedicated vulnerability reporting inbox (Section 3).
2. The exact URL of the website compliance page (Section 3).
3. The final number of days for the default coordinated-disclosure remediation window (Section 6).

Signature record

Role	Name	Signature	Date
Prepared by	Jin Cancan		2026-09-03
Reviewed by	Zhou Yang		2026-09-03
Approved by	Zhou Yang		2026-09-03