Security Update Policy

Document No.	CRA-SUP-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 sets out the manufacturer's mechanism for providing security updates during the support period, so as to satisfy the requirements of Annex I Part II, points (2), (7) and (8) and Article 13(8) and (9) concerning free-of-charge, timely, distributable and available updates, and to remain consistent with Annex I Part I, point (2)(c) (applicability of automatic security updates).

Reference: Regulation (EU) 2024/2847, Annex I Part II, points (2), (7) and (8); Articles 13(8) and (9); Annex I Part I, point (2)(c).

2 Scope

This policy applies to security updates for the NFT software (assessed baseline version Ver 2.26.8 and later versions released during the support period), including remedies for known exploitable vulnerabilities, mitigating measures and necessary accompanying fixes.

3 Free of charge

Every security update made available to users during the support period is provided **free of charge**, except where the manufacturer and a business user have agreed otherwise for a customised product (Annex I Part II, point (8)). NFT is a one-time perpetual-licence commercial software; security updates are distributed free of charge under the licence and are not billed separately.

4 Separation from functionality updates

Where technically feasible, new security updates are provided **separately from functionality updates** (Annex I Part II, point (2)). This product uses an independent security-update release channel: security updates are released as separate builds not tied to new features; functionality-version iterations are released separately. Users may install a security update without upgrading functionality.

5 Distribution mechanism

- **Distribution channel**: published via the download area and update-notification page of the website https://www.flash-tracer.com/; users may also obtain updates through the in-product "Check for updates" function (Annex I Part II, point (7)).
- **Integrity verification**: each security update package is accompanied by a SHA-256 checksum; where feasible, code signing is used to assure authenticity and integrity of origin.

> No code-signing certificate is used; integrity is verified by MD5 checksum published on the compliance page (https://www.flash-tracer.com/about.html).

- **Timely distribution**: security updates are released without delay once they can resolve an identified security issue (Annex I Part II, point (8)).

6 Applicability of automatic updates

NFT is a locally installed, offline professional tool deployed in laboratories and digital-forensics institutions. In its use context, unattended automatic installation of updates is neither expected by users nor appropriate. Pursuant to the "where applicable" wording of Annex I Part I, point (2)(c) and Recital 56, this product does **not enable automatic installation of security updates by default**, and adopts the following alternative measures instead:

- The software includes a "Check for updates" function that issues a **clear notification to the user** when a security update is available;
- Installation is executed upon user confirmation (with an option to temporarily postpone the update);
- This mechanism is clearly explained in the user information and instructions (Annex II, points 8(c) and 8(e)), including how to turn off automatic checking (if the user chooses).

This arrangement is justified under point (2)(c) of Annex I Part I in the Cybersecurity Risk Assessment (CRA-RA-001) and confirmed by the Module A Self-Assessment (CRA-CA-001) as meeting the "where applicable" requirement of Annex I Part I, point (2)(c).

7 Availability and retention

Each security update released during the support period shall remain **available for at least 10 years after its release or the remainder of the support period, whichever is longer** (Article 13(9)). Historical security update packages and their checksums are archived in the website download area and an internal backup, ensuring users can obtain them during the support period.

8 User notification

When a security update is released, users are notified via the website announcement board, a pinned forum post and, where feasible, an email list, explaining the vulnerability impact, severity, measures users can take and the installation method (Annex I Part II, point (8) and Annex II, point 8(c)).

9 Relationship with companion documents

- Source of remediation: Vulnerability Handling Process CRA-VHP-001
- Reporting trigger: Vulnerability and Incident Reporting Procedure CRA-IRP-001
- Component inventory: CRA-SBOM-001
- Disclosure: CRA-CVD-001

10 Items pending confirmation

1. Actual configuration of the code-signing certificate and signing procedure (Section 5).
2. Specific storage location and backup strategy for archived security updates (Section 7).
3. The carrier and user-subscription mechanism for email-list notification (Section 8).

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