Nand Flash Tracer (NFT) Technical Documentation (Annex VII to Regulation (EU) 2024/2847)

Item	Content
Document number	CRA-TD-001
Version	V1.0
Date of issue	2 September 2026
Prepared by	Jin Cancan
Reviewed by	Zhou Yang
Approved by	Zhou Yang
Product covered	Nand Flash Tracer (NFT), software only, assessed baseline version Ver 2.26.8
Language	English version — Official Version for EU Market Surveillance Authorities

Note: The Chinese version of this document (CRA-TD-001 V1.0, Internal Working Version) is the internal working text. Both language versions have identical structure, section numbering, tables and compliance conclusions. The CRA does not prescribe a language for the technical documentation where no notified body is involved (this product follows Module A). The EU declaration of conformity and the user information must be provided in a language required by the Member State in which the product is made available, and in a language easily understood by users and market surveillance authorities. English is used as the official external language for this product; local language versions will be added where a specific Member State so requires.

1. Purpose and scope

1.1 Purpose

This document is the technical documentation drawn up by Dalian ByteSmart Technology Co., Ltd. in respect of its product Nand Flash Tracer pursuant to Article 31 of Regulation (EU) 2024/2847 (the Cyber Resilience Act, hereinafter "CRA"). It serves to demonstrate that the product meets the essential cybersecurity requirements set out in Annex I, Parts I and II, to the CRA and supports the conformity assessment procedure under Module A (internal production control).

Reference: Regulation (EU) 2024/2847, Article 31(1) and Annex VII; Annex VIII, Part I, point 2.

1.2 Product covered

Item	Content
Product name	Nand Flash Tracer (NFT)
Manufacturer	Dalian ByteSmart Technology Co., Ltd.
Registered address	No.32, 1st Floor, No.555 Huanghe Road, Shahekou District, Dalian City, Liaoning Province, China
Product type	Software only; locally installed data recovery and data reconstruction tool

CRA classification	Default / Standard category
Conformity assessment procedure	Annex VIII, Part I, Module A (internal production control, self-assessment, no notified body)
CRA role	Manufacturer, not established in the Union
Assessed baseline version	Ver 2.26.8

Reference: Regulation (EU) 2024/2847, Annex VIII, Part I, point 1 (the manufacturer shall, under its sole responsibility, ensure and declare that the product satisfies all essential cybersecurity requirements in Annex I, Part I, and that the manufacturer satisfies those in Annex I, Part II).

1.3 Assessed baseline version

The assessed baseline version for this technical documentation is **Ver 2.26.8**. All conclusions in this document concerning architecture, data flow, external interfaces, attack surface, security measures and the conformity mapping are based on that version.

1.4 Product boundary

The compliance conclusions set out in this document cover the following only:

1. The locally installed body of the NFT software (the installer, the main executable and its bundled runtime dependencies, the chip ID database files and the default configuration templates);
2. The update check module and the licence activation (device binding verification) module, which together constitute the product's only external network interaction;
3. The user information and instructions supplied by the manufacturer with the product (see Appendix A).

The following are expressly **outside** the product boundary and are not covered by any compliance conclusion in this document:

4. Chip reading hardware supplied by the user (third-party flash programmers or readers) together with its drivers and firmware; the manufacturer defines the import file format only and bears no responsibility for the cybersecurity of that hardware;
5. Storage media supplied by the user (USB drives, SD cards, TF cards, eMMC, SSDs and IoT storage chips) and the content of dump images generated by the user or by third parties;
6. Content published on the manufacturer's website and forum, including content published by third parties and by users;
7. The Windows operating system on which NFT runs, its file system encryption mechanisms and account model, and the perimeter protection of the user's network.

Reference: Regulation (EU) 2024/2847, Article 13(1) (manufacturer obligations relate to the product it places on the market); Annex VII, point 1 (the technical documentation shall describe the product itself).

1.5 Relationship with CRA-CLASS-001 and the version discrepancy

The first-step record "Product Scope and Classification Confirmation Record" (CRA-CLASS-001 V2.1, 24 August 2026) records the version as Ver 2.26.0617. The assessed baseline version for this set of documents is Ver 2.26.8. Both belong to the 2.26 series, the core functionality is unchanged, and the classification conclusion (Default / Standard, Module A) continues to apply. The changes in Ver 2.26.8 relative to Ver 2.26.0617 constitute routine revisions within the same version series and do not amount to a **substantial modification** within the meaning of Article 3 of the CRA.

Reference: Regulation (EU) 2024/2847, Article 3 (definition of "substantial modification"); Article 22.

1.6 Triggers for re-assessment

The manufacturer shall re-assess the classification conclusion and update this technical documentation where any of the following occurs:

8. The intended purpose of the product changes (for example, the addition of cloud processing, remote assistance or networked collaboration features);
9. A change occurs that constitutes a "substantial modification" within the meaning of Article 3, including the introduction of a new external network service, a new external interface or a new third-party component;
10. The product is reclassified as an important or critical product, or implementing acts such as (EU) 2025/2392 further specify the technical descriptions;
11. The support period expires, is extended, or is terminated early;
12. A reference to a relevant harmonised standard is published in the Official Journal of the European Union (OJEU), or the Commission adopts new common specifications;
13. A severe incident reportable under Article 14 occurs, or an actively exploited vulnerability arises that may alter the basis of the classification.

Reference: Regulation (EU) 2024/2847, Article 31(2); Article 13(3) and (7); Article 22.

1.7 Documentation set and cross-references

Document number	Title	Relationship to this document
CRA-CLASS-001	Product Scope and Classification Confirmation Record (V2.1)	Prior input; establishes the Default classification and the Module A route
CRA-TD-001	Technical Documentation (this document)	Consolidates and indexes the Annex VII elements
CRA-RA-001	Cybersecurity Risk Assessment	Annex VII, point 3; see section 9
CRA-TR-001	Test Report	Annex VII, point 6; see section 8
CRA-SBOM-001	Software Bill of Materials (SBOM)	Annex VII, points 2(b) and 8; see section 11
CRA-VHP-001	Vulnerability Handling Process	Annex VII, point 2(b); see section 4
CRA-CVD-001	Coordinated Vulnerability	Annex VII, point 2(b); see

	Disclosure Policy	section 4
CRA-SUP-001	Security Update Policy	Annex VII, point 2(b); see section 4
CRA-DoC-001	EU Declaration of Conformity	Annex VII, point 7; see section 10
CRA-CA-001	Conformity Assessment (Module A Self-Assessment) Record	Evidence of compliance with Annex VIII, Part I, point 1
CRA-CE-001	CE Marking Description	Manner of affixing for a product in the form of software, per Article 30
CRA-IRP-001	Incident and Vulnerability Reporting Procedure	Reporting obligations under Article 14
CRA-RET-001	Documentation Retention and Access Management	Evidence of retention under Article 13(13)

2. General description of the product (Annex VII, point 1)

Reference: Regulation (EU) 2024/2847, Annex VII, point 1.

2.1 Product identification

Item	Content
Product name	Nand Flash Tracer
Short name	NFT
Product type	Software only (no hardware components)
Assessed baseline version	Ver 2.26.8
Internal build identifier	Internal build identifier corresponding to Ver 3.26.8.26
Supported operating systems	Windows 7 / 10 / 11
Deployment	Local stand-alone installation; no cloud service; no remote data processing

Build identifier scheme. The manufacturer intends, from the approval of this document onwards, to apply the following build identifier scheme: **NFT-major.minor.patch-YYYYMMDD** (example: NFT-2.26.8-20260902). The identifier is written into the "About" dialogue, the installer file name and the release record, and constitutes the "other element allowing identification" required by Article 13(15). For a product that exists in the form of software and has no physical carrier for a type, batch or serial number, the combination of version number and internal build number satisfies the product identification requirement of that Article.

Reference: Regulation (EU) 2024/2847, Article 13(15).

2.2 Intended purpose (Annex VII, point 1(a))

NFT is intended for use by professional data recovery laboratories, data recovery technicians and digital forensic bodies, for parsing, virtual page re-assembly and data reconstruction of raw NAND flash dump images obtained by chip removal and reading. The intended purpose comprises:

14. Parsing dump images from USB drives, SD cards, TF cards, eMMC, consumer SSDs and IoT storage chips (automotive, unmanned aerial vehicles and similar);
15. Bad block identification, filtering and correction, with support for SLC / MLC / TLC / QLC devices;
16. XOR key detection, data offset calibration and Read-Retry, for handling encryption, page scrambling, weak blocks and incomplete dumps;
17. ECC correction checking and batch ECC processing, including parsing of the ECC status contained in the raw image;
18. Pre-processing such as sector cutting, bad byte trimming and formula conversion (including user-defined formula conversion);
19. Importing dump images produced by third-party flash reader hardware;
20. Verifying the software licence through device binding verification (issue date and device binding verification were added in the version of 23 May 2025).

Intended environment of use (security environment provided by the manufacturer): a stand-alone Windows environment (Windows 7 / 10 / 11), recommended to be deployed in a controlled physical location, run under a non-administrator account, with operating system and disk encryption enabled, and kept offline or within a controlled network when sensitive data are processed.

Uses outside the intended purpose: the product is not intended to serve as a network service, a forensic evidence preservation system, a cryptographic erasure tool or a mass storage management system. The manufacturer provides no SDK, library or redistribution interface; the product is not designed to be integrated in the form of a component.

Reference: Regulation (EU) 2024/2847, Annex VII, point 1(a); Annex II, point 4.

2.3 Software versions affecting conformity with the essential cybersecurity requirements (Annex VII, point 1(b))

Version control policy. The manufacturer applies a three-part version number (major.minor.patch; example: 2.26.8). The rules are as follows:

21. Change of major version: architectural or intended-purpose level change; requires a fresh risk assessment and may trigger the re-assessment referred to in section 1.6;
22. Change of minor version: functional change that may affect external interfaces, dependencies or the attack surface; requires an update of the SBOM and the application of the pre-release security gate (see section 5.3);
23. Change of patch level: defect fixes and security fixes; subject to regression testing and the security update process (see section 4).

Version series covered by the compliance conclusions of this document.

Version series	Status	Within the scope of the compliance conclusions
2.26 series (including Ver 2.26.0617 and the assessed baseline version Ver 2.26.8)	Current	Yes (assessed baseline for this document)

Subsequent patch versions within the 2.26 series	Future releases	Yes, provided that the pre-release security gate in section 5.3 is passed and no change of intended purpose occurs
Series 2.25 and earlier	No longer distributed	No; no further functional updates, security fixes only during the remainder of their support period (see section 6)

Note: The manufacturer does not claim a continuing conformity conclusion for historical versions that are no longer distributed. However, in accordance with Article 13(8) to (10), vulnerabilities in those versions continue to be handled in a reasonable manner during the support period.

Reference: Regulation (EU) 2024/2847, Annex VII, point 1(b); Article 13(8) and (10).

2.4 Photographs or illustrations of hardware (Annex VII, point 1(c)) — not applicable

The product is **software only** and contains no hardware components. The photographs or illustrations of hardware required by Annex VII, point 1(c) are therefore **not applicable**. Product identifiability is achieved through the product identification information in section 2.1 (product name, version, build identifier).

Reference: Regulation (EU) 2024/2847, Annex VII, point 1(c) (that point applies to hardware products only); Article 13(15).

2.5 User information and instructions (Annex VII, point 1(d))

The **complete publishable text** of the user information and instructions supplied with the product is set out in **Appendix A** to this document and covers all the requirements of Annex II, points 1 to 9, to the CRA. That text is supplied in electronic form with the installer (under the title "User Information and Security Instructions") and is published on the manufacturer's website.

Reference: Regulation (EU) 2024/2847, Annex VII, point 1(d); Annex II; Article 13(18).

3. Design, development and production of the product (Annex VII, point 2(a))

Reference: Regulation (EU) 2024/2847, Annex VII, point 2(a).

3.1 System architecture

NFT employs a layered architecture. The responsibilities of each layer and the manner in which the components build on, or feed into, one another are as follows:

Layer	Component	Main responsibility	Feeding relationship
1	User interface layer	Job and project management, parameter configuration wizard, result visualisation, progress and log	Calls the job interface of layer 2; does not access file parsing logic directly

		display	
2	Job / project and layout configuration layer	Project file read and write, job parameters and page/block layout configuration management, job state persistence	Issues configuration and scheduling instructions to layers 3, 5, 6, 7 and 8
3	Dump image input/output layer	Import of image files produced by chip readers, format validation, export of reconstructed images and project data	Receives parameters from layer 2; outputs raw data streams to layers 4 to 9
4	Chip ID database	Matching of die model, page/block size and default layout on the basis of chip identifiers and signatures in the dump	Queried by layer 5; updated with each release
5	Page/block layout and virtual page re-assembly engine	Inference and application of page/block layout; virtual page re-assembly and page de-scrambling	Consumes the data stream of layer 3 and the parameters of layer 4; outputs to layers 6 and 7
6	ECC analysis and batch ECC processing module	Parsing of ECC status in the raw image; correction checking and batch processing	Consumes the output of layer 5; returns correctable/uncorrectable status to layer 2
7	XOR key detection and de-scrambling module	XOR key detection, data offset calibration and de-scrambling; handling of Read-Retry and weak blocks	Consumes the output of layers 5 and 6
8	Sector cutting / bad byte trimming / formula conversion module	Pre-processing: sector cutting, bad byte trimming and user-defined formula conversion	Consumes the output of layer 7; supports a restricted expression evaluator
9	Bad block management module	Bad block identification, filtering and correction; maintenance of the bad block table	Spans layers 5 to 8; reports statistics and anomalies to layer 2
10	Licence activation and device binding module	Licence verification, issue date verification, device binding verification; the product's only external network interaction	Invoked at start-up or when triggered by the user; the result is written to the local licence state
11	Update check	Checking for and	Triggered by the user or

	module	downloading available updates; verification of update package integrity and origin	by the default policy; see section 4.3

Note: The layered description above constitutes the "description of the system architecture showing how software components build on or feed into each other and integrate into the overall processing" required by Annex VII, point 2(a). Layers 1 to 9 form the offline data processing chain; layers 10 and 11 are ancillary network-facing components.

3.2 Data flow

The complete data flow from dump import to reconstructed output is as follows:

24. The user selects a local dump image file in layer 1; layer 3 performs format allow-listing, file header and size validation, and rejects input that does not match the expected structure with an explicit error message;
25. Layer 3 reads the image block by block and passes it to layer 4, which identifies or matches the chip identifier in order to determine candidate page/block layouts;
26. The user may confirm or manually adjust the layout parameters in layer 2; layer 5 then performs virtual page re-assembly and page de-scrambling on that basis;
27. Layer 6 parses the ECC status and performs batch correction; uncorrectable pages are flagged as anomalies and returned to layer 2;
28. Layer 7 performs XOR key detection, offset calibration and de-scrambling, and handles Read-Retry and weak block data;
29. Layer 9 applies the bad block table to perform filtering and correction;
30. Layer 8 performs sector cutting, bad byte trimming and formula conversion according to the user's configuration;
31. Layer 3 writes the reconstruction result to the user-specified output directory (a standard image file) and saves the project file;
32. A job log is generated throughout in layer 2, for user traceability and troubleshooting.

Note: The entire flow is completed locally. There is no data upload, no cloud processing and no remote computation. The software does not retain personal data or sensitive data recovered by the user; image data are processed entirely on the local machine.

3.3 External interfaces and the resulting attack surface

External interface	Direction	Nature	Main threats	Mitigations implemented
Dump image file import	Inbound (local file)	**Principal external untrusted input**	Out-of-bounds read/write, integer overflow and resource exhaustion caused by malformed files (decompression bombs, oversized images)	Format allow-listing, header and structure validation, strict bounds checking, input size limits, safe fallback on import failure, fuzz testing of the parsing path (see CRA-TR-

				001)
Project file and layout configuration file import	Inbound (local file)	Semi-trusted (locally generated)	Deserialisation flaws, out-of-range fields	Structured parsing, field type and value range validation, file format version marking and compatibility checks
User-defined formula input	Inbound (user input)	Semi-trusted	Expression injection, resource exhaustion during evaluation	A restricted expression evaluator is used, with no file system, process or network access; limits on evaluation time and iteration count
Output file and project file write	Outbound (local file)	User controlled	Path traversal, unintended overwrite	Output directory explicitly specified by the user; output paths containing relative traversal segments are rejected; confirmation required before overwriting existing files
Licence activation and device binding	Outbound (HTTPS)	**Only network interaction**; triggered by the user or at start-up	Man-in-the-middle attack, forged server response, flaws in response field parsing	Outbound HTTPS only, server certificate verification, strict parsing of response fields, anomalous responses treated as failure
Update check and download	Outbound (HTTPS)	Triggered by the user or by the default policy	Forged update package, downgrade attack	Download from official channels only; verification of update package integrity and origin (see section 4.3); version monotonicity check
Inbound listening ports	None	Not applicable	Not applicable	The product opens no inbound listening port, does not run as a system service, and

				does not listen on local sockets awaiting external connections

Domain name: www.flash-tracer.com

Transmitted activation content: Activation Code

Conclusion on the attack surface. The effective attack surface of NFT is concentrated in the "dump image file import parsing path", followed by "licence activation response parsing" and "update package verification". The product has no inbound listening port, no remote data processing and no cloud component, and therefore presents no network-facing remote attack surface.

Reference: Regulation (EU) 2024/2847, Annex I, Part I, point (2)(j) (limit the attack surface, including external interfaces, in design, development and production).

3.4 Secure-by-design and secure-by-default principles applied, and their mapping to Annex I, Part I

The manufacturer applies the following principles in design and development, mapped to the relevant essential requirements in Annex I, Part I:

Principle	Implementation	Mapping
Data localisation	All image parsing and reconstruction is performed locally; no upload, no cloud processing, no telemetry	Points (2)(e) and (g)
Data minimisation	Only files explicitly selected by the user are read; activation transmits licence and device identifier fields only; no personal data are collected	Point (2)(g)
Minimum attack surface	No inbound listening port; does not reside as a service; the only network interaction is licence activation, which is perceptible to the user	Points (2)(i) and (j)
Untrusted input	The import path applies format allow-listing, structure validation, bounds checking and size limits; user-defined formulas use a restricted evaluator	Points (2)(j) and (k)
Secure by default	Data processing is not networked by default; diagnostic data return is disabled by default; the default output directory is the user directory and existing files are not overwritten	Point (2)(b)
Integrity first	The ECC/checksum status of dumps and the structure of	Point (2)(f)

	project files are verified and corruption reported; update packages are checked for integrity and origin	
Due diligence on third-party components	An SBOM is maintained; dependencies are scanned for known vulnerabilities before release; actively maintained components are preferred	Point (2)(a); Article 13(5)
Recoverability	Job state is persisted so that jobs can be resumed after an abnormal interruption; long-running tasks can be cancelled	Point (2)(h)

Reference: Regulation (EU) 2024/2847, Annex I, Part I, point (1) (products shall be designed, developed and produced to ensure an appropriate level of cybersecurity based on risks) and the points of paragraph (2); Article 13(2) and (5).

4. Vulnerability handling processes (Annex VII, point 2(b))

Reference: Regulation (EU) 2024/2847, Annex VII, point 2(b); Annex I, Part II; Article 13(8).

4.1 Processes established and related documents

Requirement	Corresponding process/document	Document number
Identify and document vulnerabilities and components, including the SBOM	Software bill of materials and component vulnerability monitoring mechanism	CRA-SBOM-001
Handle and remediate vulnerabilities without delay and provide security updates	Vulnerability handling process	CRA-VHP-001
Security update policy (release, availability, separation from functionality updates)	Security update policy	CRA-SUP-001
Coordinated vulnerability disclosure policy	Coordinated vulnerability disclosure policy	CRA-CVD-001
Effective and regular testing and review	Test report and annual review	CRA-TR-001
Risk identification and applicability determination	Cybersecurity risk assessment	CRA-RA-001
Reporting of actively exploited vulnerabilities and severe incidents	Incident and vulnerability reporting procedure	CRA-IRP-001

4.2 Contact address for reporting vulnerabilities and evidence that it has been provided

Item	Content

Contact address for reporting vulnerabilities (email)	nandflashtracer@gmail.com
This address also serves as	The **single point of contact** required by Article 13(17)
Means of consulting the coordinated vulnerability disclosure policy	Published on the website notices and as a pinned forum post (full text of CRA-CVD-001); also available on request by email
Alternative communication channels	Manufacturer website https://www.flash-tracer.com/ and forum https://www.flash-tracer.com/bbs/forum.php
Evidence that it has been provided	Vulnerability reporting page: https://www.flash- tracer.com/about.html Initial publication date: September 3, 2026

Note: Article 13(17) requires the single point of contact to be easily identifiable, to be included in the user information and instructions, and to allow users to choose their preferred means of communication and not to be limited to automated tools. The manufacturer uses email as the principal channel and does not rely on a mandatory web form as the sole entry point, which satisfies that requirement. Reporting to the coordinated CSIRT and to ENISA under Article 14 is submitted through the single reporting platform; the procedure is set out in CRA-IRP-001.

Reference: Regulation (EU) 2024/2847, Article 13(17); Annex I, Part II, points (5) and (6); Annex VII, point 2(b) (evidence of the contact address provided for reporting vulnerabilities).

4.3 Technical solution chosen for the secure distribution of updates

Element	Solution
Distribution channel	The manufacturer's official download channel (download page on the official website) and the in-product "Check for updates" module; third-party download sites and mirror sites are not used as sources of security updates
Transport protection	Download over HTTPS (TLS) throughout; update check requests are outbound only and no inbound port is opened
Integrity verification	A SHA-256 checksum is provided for the update package and published on the download page;
Origin verification	Update packages are obtained only from the official domain; a version monotonicity check is performed before installation to prevent downgrading
Separation of security updates from functionality updates	Where technically feasible, security fixes are released as separate patch-level versions and are not bundled with functional changes; they are combined only where the fix is closely coupled to a functional change in the same code area and cannot technically be separated, in which case the release notice explains this
Notification channels	Website notice board, forum announcement, in-product update notification; known affected users are informed by email
Automation of distribution	Automatic update function is not available.

Cost	Security updates are provided free of charge (requirement (8)); functional updates follow the existing licence policy

Reference: Regulation (EU) 2024/2847, Annex I, Part II, points (2) (where technically feasible, new security updates shall be provided separately from functionality updates), (7) (mechanisms for secure distribution of updates) and (8) (release without delay and free of charge); Annex I, Part I, point (2)(c); Article 13(9).

5. Processes for the production and monitoring of the product and their verification (Annex VII, point 2(c))

Reference: Regulation (EU) 2024/2847, Annex VII, point 2(c); Article 13(14) (procedures to ensure continued conformity of series production).

5.1 Build and packaging procedure

33. After a development branch is merged, the designated responsible person performs the build in a controlled build environment;
34. The build identifier (see section 2.1) is written into the build output automatically and a version manifest is generated;
35. The installer is packaged, together with the user information and instructions file (text of Appendix A);
36. SHA-256 checksums are calculated for the installer and the main executable files;
37. The output then passes through the pre-release security gate described in section 5.3;
38. Once the gate is passed, the package is uploaded to the official download channel and the release record is updated.

Compiler version: VS2022.

Build environment: Windows 11, which is not connected to the network.

5.2 Source code control and change management

39. All source code and build scripts are placed under version control;
40. Changes are recorded as commits; security-related fixes are marked in the commit message and matched to the corresponding release notice;
41. Released versions are tagged, with the tag corresponding to the external version number;
42. Access rights are granted on a least-necessary basis.

Source code version control is implemented via SVN. The password is known only to the administrator and the person-in-charge, with minimum-scope access control applied.

5.3 Pre-release security gate (checklist)

Every version intended for release, including patch-level security updates, must satisfy each of the following items before release:

No.	Check item	Acceptance criterion	Evidence
1	Scanning of dependencies for known vulnerabilities	No unresolved high-risk items; where present, a mitigation statement is recorded	Scan record in CRA-SBOM-001
2	Regression and fuzz testing of the import parsing path	No residual test case causing a crash, out-of-bounds condition or uncontrolled resource consumption	CRA-TR-001
3	Disposition of static analysis results	High-severity warnings cleared, or a reason recorded for each one	Build record
4	Integrity verification of the update package	Checksums generated and published	Release record
5	Review of changes to the licence activation and update check modules	Any change involving network interaction undergoes a dedicated review	Review record
6	Synchronisation of user information and instructions	The text of Appendix A is updated with the version and distributed with the installer	Installer content list
7	Confirmation of attack surface changes	Any new external interface or dependency requires an update of section 3.3 and of this document	Version record of this document
8	Consistency of support period information	The support period end date shown in the product and on the website is consistent	Release record

5.4 Version and build numbering

The external version number uses three parts (major.minor.patch; see section 2.3); the internal build identifier uses the format **NFT-major.minor.patch-YYYYMMDD**. The two correspond one-to-one in the release record and can be traced back to the source code tag and the build output.

Reference: Regulation (EU) 2024/2847, Article 13(15).

5.5 Distribution channels

43. The official download page on the manufacturer's website https://www.flash-tracer.com/ (principal channel);
44. The in-product "Check for updates" module (update distribution);

45. The manufacturer's forum at https://www.flash-tracer.com/bbs/forum.php, used as an announcement channel.

5.6 Integrity protection of delivered binaries

Measure	Status
SHA-256 checksum published with each release	Implemented
Code signing (Authenticode)	No functions require this mechanism.

5.7 Release records

For each release the manufacturer retains the following records: version number and build identifier, build date, release type (security update / functionality update / combined), checksums, results of the security gate checks, text of the release notice, and the list of known issues. The manufacturer does not distribute security updates through third-party download sites. Release packages are backed up on an offline backup machine, which is not connected to the network. Only the administrator knows the system password.

6. Support period information (Annex VII, point 4)

Reference: Regulation (EU) 2024/2847, Annex VII, point 4; Article 13(8).

6.1 Support period

Item	Content
Support period	**10 February 2024 to 10 February 2029**
Duration	5 years
Commitments during the support period	Effective handling of vulnerabilities in accordance with Annex I, Part II; provision of security updates free of charge; provision of the technical support described in Appendix A, item 7
Availability of security updates	Each security update remains available for at least 10 years after its release, or for the remainder of the support period, whichever is longer

Reference: Regulation (EU) 2024/2847, Article 13(8) (support period of at least 5 years) and Article 13(9).

6.2 Factors taken into account in determining the support period (Article 13(8))

Factor	Consideration specific to this product
Reasonable expectations of users	The target users are professional data recovery laboratories and forensic bodies, which expect an availability period of approximately 5 years, consistent with the renewal cycle of their equipment and software
Nature and intended purpose of the product	Software-only local tool whose functionality depends on continuing maintenance of chip model and page/block layout knowledge, requiring sustained manufacturer investment
Expected time of use of the product	Commercial software licensed on a one-off

	perpetual basis; users expect a usage cycle of approximately 5 years
Relevant Union law	The product is not covered by sectoral Union legislation imposing a longer support obligation
Speed of technological turnover	Storage chip generations typically turn over in less than 5 years, and the software must continuously adapt to new chip generations; beyond 5 years the feasibility and effectiveness of continued maintenance decline significantly
Business model	One-off perpetual licence, with no ongoing subscription revenue to support indefinite support

Reference: Regulation (EU) 2024/2847, Article 13(8).

6.3 Communication of the end date at the time of purchase (Article 13(19))

The manufacturer states the support period end date clearly and in an easily accessible manner at the time of purchase, indicating **at least the month and the year (February 2029)**, through the following means:

46. The product page and the purchase page on the official website state "Support period until February 2029";
47. The order confirmation page and the order confirmation email repeat that statement;
48. The "About" dialogue in the software displays the support period end date.

The software is licensed for perpetual use; no expiration prompt is required.

Reference: Regulation (EU) 2024/2847, Article 13(19).

6.4 Notification shown to users when the support period ends

When the support period expires, the manufacturer displays the following notification to users within the software (a Chinese version is provided alongside it):

> ***Notice: the support period for this product (Nand Flash Tracer) ended on 10 February 2029.*** *From that date the manufacturer no longer guarantees the provision of security updates or the handling of vulnerabilities. Continued use of this software may expose you to cybersecurity risks for which you assume responsibility. It is recommended that you keep the operating environment offline, process non-sensitive data only, or upgrade to a supported version. Information on the archive of historical versions and on the risks of their use is available at: https://www.flash-tracer.com/*

Reference: Regulation (EU) 2024/2847, Article 13(19), second sentence (where technically feasible, users shall be shown a notification that the support period has expired) and Article 13(11) (information on the risks of using unsupported software held in a public software archive).

7. Standards and solutions applied (Annex VII, point 5)

Reference: Regulation (EU) 2024/2847, Annex VII, point 5.

7.1 Status of harmonised standards

Item	Status as at 2 September 2026
CRA harmonised standards	**No reference to a CRA harmonised standard has been published in the Official Journal of the European Union (OJEU)**
Standardisation request	Standardisation request M/606 entrusts CEN/CENELEC/ETSI with the development of 41 standards (including the EN 40000 series), which are still under development
List of harmonised standards applied	None
Common specifications under Article 27	None
European cybersecurity certification scheme adopted pursuant to (EU) 2019/881	None

*Important note: **the EN 18031 series consists of harmonised standards supporting the Radio Equipment Directive (RED, Directive 2014/53/EU) and is not related to the CRA.** It is not referenced for this product.*

7.2 Statement on the presumption of conformity

As at the date of issue of this document (2 September 2026) **no reference to any CRA harmonised standard has been published in the Official Journal of the European Union**. The manufacturer therefore **does not claim** the presumption of conformity under Article 27. The product has been assessed directly against the essential cybersecurity requirements in Annex I, Parts I and II, and the compliance conclusions are drawn by the manufacturer under its sole responsibility (Module A).

Reference: Regulation (EU) 2024/2847, Article 27; Annex VII, point 5; Annex VIII, Part I, point 1.

7.3 Alternative solutions adopted to meet the essential requirements in Annex I, Parts I and II

The manufacturer has adopted the following alternative solutions. The items below **constitute references to methods and industry practice only and do not amount to any certification or claim of formal conformance**:

Area	Solution adopted	Technical specification or industry practice referenced	Certification or formal conformance claimed
Secure development process	Layered architecture review, code review, pre-release security gate, change review	General practices of secure software development frameworks (SSDF-type)	**No**
Weakness awareness	Common weakness lists used as a checklist for coding	CWE Top 25 and SANS Top 25 weakness lists used	**No**

	and review (with emphasis on input validation, memory safety, path handling and deserialisation)	as reference	
Vulnerability severity rating	The Common Vulnerability Scoring System is used to rate severity and prioritise remediation	CVSS v3.1 (migration to v4.0 to be assessed)	**No**
Component inventory	SBOM drawn up in a commonly used, machine-readable format, covering at least the top-level dependencies	SPDX 2.3 (JSON); ISO/IEC 5962	**No**
Test methods	Fuzz testing of the import parsing path, static analysis, dependency vulnerability scanning, verification of the installation and update flows	Generally accepted industry test methods	**No**
Risk management method	Asset-threat-impact qualitative risk matrix, covering design, development, production, delivery and maintenance	General risk management approach of ISO/IEC 27005 used as reference (**method only; no claim of ISO/IEC 27001 certification**)	**No**
Security of update distribution	HTTPS transport plus SHA-256 checksum (code signing under evaluation) plus restriction to official channels plus version monotonicity check	See section 4.3	**No**
Data protection	Local data processing, no telemetry, no collection of personal data, reliance on the operating system for encryption at rest	See section 3.4	**No**

Reference: Regulation (EU) 2024/2847, Annex VII, point 5 (where harmonised standards, common specifications or certification schemes have not been applied, a description of the solutions adopted to meet the essential requirements in Annex I, Parts I and II, including a list of other relevant technical specifications applied).

7.4 Commitment to monitor and re-assess

The manufacturer commits to:

49. Continuously monitoring the publication of references to CRA harmonised standards in the Official Journal of the European Union, with particular attention to standardisation request M/606 and the EN 40000 series;
50. Monitoring the formal adoption of Commission CRA guidance C(2026) 5252 final and the availability of its language versions;
51. Completing a gap assessment within **6 months** of the publication in the OJEU of a reference to a relevant harmonised standard or common specification, and updating sections 7.1 and 7.3 and Appendix B accordingly, together with the risk assessment (CRA-RA-001) and the EU declaration of conformity (CRA-DoC-001) where necessary;
52. Assigning responsibility for that monitoring to the release and documentation owner referred to in section 5.7, and including it in the annual review described in section 12.

Reference: Regulation (EU) 2024/2847, Annex VII, point 5; Article 31(2).

> *Note: The manufacturer is a micro/small enterprise and is not in a position to operate a 24/7 security operations centre, to obtain ISMS certification or to run a bug bounty programme. The commitments above are set at a scale that can actually be implemented.*

8. Testing (Annex VII, point 6)

The tests carried out by the manufacturer to verify that the product and the vulnerability handling processes meet the applicable essential requirements in Annex I, Parts I and II, are consolidated in the Test Report, CRA-TR-001; the details of those tests are not repeated in this document. The test scope includes at least:

53. Robustness testing of the import parsing path (fuzz testing and regression testing with malformed and out-of-range image files);
54. Static analysis results and their disposition;
55. Results of scanning dependencies for known vulnerabilities;
56. Verification of the installation, update check and update package verification flows;
57. Verification of the network interaction and anomalous response handling of the licence activation module;
58. Verification that the user information and instructions are supplied, that the support period end date is displayed, and that it is stated at the time of purchase;
59. Results of exercises of the vulnerability handling process itself (end-to-end exercise from receipt of a report to release of an update).

Finalization date: September 3, 2026. Assessment result: No risk.

Reference: Regulation (EU) 2024/2847, Annex VII, point 6; Annex I, Part II, point (3) (effective and regular testing and review of the security of the product).

9. Cybersecurity risk assessment (Annex VII, point 3)

The manufacturer has carried out a cybersecurity risk assessment pursuant to Article 13(2) to (4); its full content is set out in the Cybersecurity Risk Assessment, CRA-

RA-001. That assessment covers the design, development, production, delivery and maintenance stages and satisfies the following requirements:

60. It is based on an analysis of risks arising from the intended purpose and from reasonably foreseeable use and conditions of use (operating environment, assets to be protected), and takes account of the expected time of use of the product;
61. It **indicates, for each of the security requirements in Annex I, Part I, point (2), whether that requirement applies and how it has been implemented**, and explains how point (1) of Part I and the vulnerability handling requirements of Part II apply;
62. It gives an explicit justification for each essential requirement that is **not applicable** (Article 13(4));
63. It is included in the technical documentation and updated as appropriate during the support period.

Appendix B to this document sets out, in tabular form, the applicability, measures implemented, supporting evidence and conclusion for each of the requirements in Annex I, Part I, point (2) (points (a) to (m)) and Part II (points (1) to (8)). Appendix B and CRA-RA-001 are consistent; in the event of any inconsistency, CRA-RA-001 prevails and this document is revised accordingly.

Test date: August 27, 2026. Test result: Meets requirements. Test results shall be updated if relevant content is adjusted subsequently.

Reference: Regulation (EU) 2024/2847, Annex VII, point 3; Article 13(2), (3), (4) and (7).

10. EU declaration of conformity (Annex VII, point 7)

The manufacturer has drawn up a written EU declaration of conformity pursuant to Article 28, bearing document number **CRA-DoC-001**. Its wording follows the template structure of Annex V and contains the elements required by Annex VIII, Part I, point 4.2. That declaration:

64. States that conformity with the applicable essential requirements of Annex I has been demonstrated;
65. Is supplied with the product (or the accompanying documents state the exact internet address at which the full declaration can be consulted);
66. Is kept together with the technical documentation and made available to national authorities for 10 years after the product has been placed on the market, or for the support period, whichever is longer;
67. Is updated as appropriate and provided in the language required by the Member State in which the product is made available.

This product follows Module A and no notified body is involved in the conformity assessment. Consequently, the EU declaration of conformity contains **no name or identification number of a notified body**, and **no notified body identification number** is added after the CE marking.

Date of issue of CRA-compliance declaration: September 3, 2026

Publication address: www.flash- tracer.com

Reference: Regulation (EU) 2024/2847, Annex VII, point 7; Article 28; Annex V; Annex VIII, Part I, point 4.2; Article 13(12), (13) and (20); Article 30(4).

11. Software bill of materials (Annex VII, points 2(b) and 8)

Item	Content
Document number	CRA-SBOM-001
Format	SPDX 2.3, JSON encoding (a commonly used, machine-readable format)
Coverage	At least the top-level dependencies of the product, to be extended progressively to deeper levels
Update frequency	Updated before each external release; mandatory for minor version changes and above
Update triggers	Addition, removal or upgrade of a third-party component; discovery of a vulnerability in a component; upgrade of the SBOM format version; request from a market surveillance authority
Retention	Archived with the release records and retained together with the technical documentation (Article 13(13))
Public availability	**Not published by default**
Manner of provision	Provided upon a **reasoned request** from a market surveillance authority, where that request is necessary to verify conformity with the essential requirements of Annex I, and in a format and language that can be understood

Date of issue: September 3, 2026

Internet address: https://tracer.com/about.html

Reference: Regulation (EU) 2024/2847, Annex VII, points 2(b) and 8; Annex I, Part II, point (1); Article 13(5) and (22).

12. Documentation control and maintenance

12.1 Continuous updating

This technical documentation has been drawn up before the product is placed on the market and will be **continuously updated as appropriate, at least during the support period**.

Reference: Regulation (EU) 2024/2847, Article 31(2); Article 13(12).

12.2 Retention period

This technical documentation and the EU declaration of conformity are kept **for at least 10 years after the product has been placed on the market, or for the support period, whichever is longer**, and are made available to market

surveillance authorities. The accompanying user information and instructions are retained for the same period; where provided online, they remain accessible online for the same period.

The support period for this product ends on 10 February 2029. Calculated on the basis of "10 years after placing on the market or the support period, whichever is longer", this document is expected to be retained until no earlier than 2036 (counting from the actual date of placing on the market).

First placing- on- the- market date: February 10, 2024

Reference: Regulation (EU) 2024/2847, Article 13(13) and (18); Annex VIII, Part I, point 4.2.

12.3 Change triggers

Trigger	Content to be updated
A change constituting a "substantial modification" within the meaning of Article 3	Sections 2, 3 and 9 and Appendices A and B; reclassification where necessary (CRA-CLASS-001)
Change of intended purpose	Section 2.2, Appendix A item 4, risk assessment (CRA-RA-001)
Addition or replacement of a third-party component	Section 11, CRA-SBOM-001
Addition of an external interface or network interaction	Section 3.3, Appendix B
Occurrence of a security incident or an actively exploited vulnerability	Section 4, CRA-RA-001, CRA-TR-001
Publication in the OJEU of a reference to a relevant harmonised standard or common specification	Section 7, Appendix B, CRA-DoC-001
Extension, shortening or expiry of the support period	Section 6, Appendix A item 7
Change of manufacturer name, address or point of contact	Information table, Appendix A items 1 and 2, CRA-DoC-001

12.4 Version records

Version	Date	Prepared by	Reviewed / approved by	Main changes
V1.0	2 September 2026	Jin Cancan	Zhou Yang	First issue; assessed baseline version Ver 2.26.8; consistent with the classification conclusion of CRA-CLASS-001 V2.1 (Default, Module A)

12.5 Storage and access

Document storage location: https://www.flash-tracer.com/about.html

Person responsible for reading: Zhou Yang

Regular monthly backup to the data machine.

Appendix A User information and instructions (Annex II, points 1 to 9)

The text below is supplied with the product and is intended for publication. Reference: Regulation (EU) 2024/2847, Annex II; Article 13(18).

A.1 Manufacturer identity and contact details (Annex II, point 1)

Manufacturer: Dalian ByteSmart Technology Co., Ltd. / 大连比特智序科技有限公司

Registered address: No.32, 1st Floor, No.555 Huanghe Road, Shahekou District, Dalian City, Liaoning Province, China

Telephone: +86 15524692190

Email: nandflashtracer@gmail.com

Website: https://www.flash-tracer.com/

Forum / community: https://www.flash-tracer.com/bbs/forum.php

A.2 Single point of contact (Annex II, point 2)

Single point of contact: nandflashtracer@gmail.com

This point of contact serves for reporting information on vulnerabilities discovered or present in the product, for receiving replies concerning vulnerabilities, and for requesting or consulting the company's Coordinated Vulnerability Disclosure Policy (CRA-CVD-001, published on the website notice board and as a pinned forum post).

You may contact us using the means of communication you prefer (email, the contact facility on the website, or a private message on the forum). We do **not** rely on any automated tool, such as a mandatory web form or a chatbot, as the only means of contact. Reports concerning security vulnerabilities will be acknowledged within **3 working days**.

A.3 Product name, type and identification (Annex II, point 3)

Product name: Nand Flash Tracer (NFT)

Product type: software-only product (a locally installed Windows desktop application); contains no hardware components

Version: Ver 2.26.8.26

Build identifier:NFT-2.26.8-20260826

Supported operating systems: Windows 7 / 10 / 11

A.4 Intended purpose, security environment and security properties (Annex II, point 4)

Intended purpose. NFT is intended for use by professional data recovery laboratories, data recovery technicians and digital forensic bodies, for parsing, virtual page re-assembly and data reconstruction of raw NAND flash dump images obtained

by chip removal and reading. It supports data from USB drives, SD cards, TF cards, eMMC, consumer SSDs and IoT storage chips (automotive, unmanned aerial vehicles and similar), and provides bad block identification and correction, XOR key detection and de-scrambling, ECC correction checking and batch ECC processing, sector cutting, bad byte trimming and formula conversion.

Security environment provided by the manufacturer. The product is designed for use in a **stand-alone, local, offline-first** environment:

68. Install and run it on a dedicated Windows host located in a controlled physical area;
69. Run day-to-day jobs under a **non-administrator (standard user) account**;
70. Keep operating system security updates and anti-malware protection enabled;
71. When processing sensitive data, use the disk encryption provided by the operating system (for example BitLocker) and keep the host network-isolated or within a controlled network during processing;
72. Obtain installation packages and updates only from the manufacturer's official channels.

Basic functionality. See "Intended purpose" above in this item A.4.

Security properties.

Security property	Description
Data localisation	All image parsing and reconstruction is performed locally; no data upload, no cloud processing, no remote computation
No telemetry	No collection of usage behaviour and no collection of personal data
Network interaction	Licence activation and update checks are performed only when triggered by the user or at start-up, and are both **outbound HTTPS** connections
No inbound ports	The product opens no inbound listening port and does not reside as a system service awaiting connections
Update integrity	A SHA-256 checksum is provided for update packages (and, once code signing is adopted, a signature is verified); updates are obtained only from official channels
Licence binding	Since the version of 23 May 2025, issue date and device binding verification are provided, preventing the licence from being copied to unauthorised devices

A.5 Known or foreseeable circumstances that may lead to significant cybersecurity risk (Annex II, point 5)

When the product is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, the following circumstances may give rise to a **significant cybersecurity risk** and should be avoided by users:

73. **Importing dump images or project files of unknown origin.** The parsing path for images and project files is the principal external input to this product, and an

attacker may construct a malformed file to exploit it. Import only files that you have generated yourself or that come from a trusted source, and scan them for malware before processing.

74. **Using installation or update packages obtained from non-official channels.** Third-party download sites may supply tampered installation packages.
75. **Running the product on a compromised or unpatched host.** The product cannot protect against risks residing in its host operating system.
76. **Not installing security updates for a prolonged period, or disabling update checks.** This leaves known vulnerabilities unremediated.
77. **Running with administrator privileges and opening project files of unknown origin.**
78. **Processing images containing personal or sensitive data on an unencrypted, shared or networked host.** The product does not encrypt local files; the confidentiality of data at rest depends on the operating system configuration.
79. **Improper use of the user-defined formula conversion function.** Use only formulas whose meaning you understand; formulas obtained from third parties may consume substantial system resources.

A.6 Internet address of the EU declaration of conformity (Annex II, point 6)

The EU declaration of conformity for this product (CRA-DoC-001) can be consulted at:

Date of issue of CRA- compliance declaration: September 3, 2026

Publication address: www.flash- tracer.com

A.7 Type of technical security support offered and the end date of the support period (Annex II, point 7)

Support period: 10 February 2024 to **February 2029** (support period end date: 10 February 2029)

Types of technical security support offered:

80. **Vulnerability intake and handling:** vulnerability reports are received at nandflashtracer@gmail.com, acknowledged within 3 working days, and processed according to severity;
81. **Security updates:** provided free of charge during the support period; each security update remains available for at least 10 years after its release, or for the remainder of the support period, whichever is longer;
82. **Security advisories:** information on remediated vulnerabilities (description, affected versions, impact, severity and remediation guidance) is published on the website notice board and the forum;
83. **Usage support:** installation, configuration and usage support is provided by email and through the forum (in Chinese and English, on working days, with a

first reply targeted within 3 working days on a best-efforts basis; no 24/7 response is offered);

84. **Documentation:** continuously updated versions of these user information and instructions are provided.

    After the end of the support period, the manufacturer no longer guarantees the provision of security updates or the handling of vulnerabilities; the cybersecurity risks of continued use are borne by the user. Users will receive a notification within the software when the support period has expired.

A.8 Detailed instructions (Annex II, point 8)

(a) Measures necessary for initial commissioning and for secure use throughout the lifetime of the product

85. Download the installation package only from the official website https://www.flash-tracer.com/ and, before installing, verify the published SHA-256 checksum (once code signing is adopted, verify the validity of the digital signature);
86. Install on a dedicated Windows host with operating system security updates applied; run day-to-day jobs under a standard user account and elevate privileges only where required for installation and licence activation;
87. When processing sensitive data, enable disk encryption and keep the host network-isolated or within a controlled network during processing;
88. After first run, check the update policy in the settings and keep notifications of available updates enabled;
89. Import only dump images and project files from trusted sources, and scan imported files for malware;
90. Back up project files and output results regularly, storing backups separately from the main working environment;
91. Continue to install operating system security updates and security updates for this product throughout the lifetime of use.

(b) How changes to the product affect data security

92. An upgrade at minor version level or above may change the project file format, the default output path or third-party dependencies; back up project files before upgrading and check the output path settings afterwards;
93. Changing the default output directory to an unencrypted location (such as a shared directory or removable media) reduces the confidentiality of the output data;
94. Changing the update check or automatic update settings delays the arrival of security fixes and lengthens the exposure window for known vulnerabilities;
95. Using user-defined formula conversion changes the content and structure of the output data and may produce unexpected results; validate on a small sample before applying it to production jobs;
96. After uninstalling or downgrading this product, older project files may not be readable by the new version; export final results before changing versions.

(c) How to install security-relevant updates

97. **Method 1 (within the product):** select "Help — Check for updates" in the software menu and follow the prompts to download and install;
98. **Method 2 (manual):** obtain the latest installation package from the official download page, verify the SHA-256 checksum and install over the existing installation;
99. Security-relevant patch-level versions are announced simultaneously on the website notice board and the forum, stating the affected versions, the impact and the severity;
100. Security updates are provided **free of charge**;
101. **Turning off the default setting for the automatic installation of security updates:** No automatic update function is configured.. After turning it off, you will still receive notifications of available updates and can choose when to install them.

(d) Secure decommissioning of the product, including how to securely remove user data

102. Uninstall Nand Flash Tracer through "Apps and features" in Windows;
103. After uninstalling, manually delete any remaining project files, job logs and output directories (see below for default locations);
104. Uninstallation only requires deleting the program folder; no files exist in other locations.;
105. For dump images, cached images and output images containing personal or sensitive data, use a reliable erasure tool to perform secure wiping (this product does not provide a data erasure function);
106. Licence activation records and device binding information are stored locally and are removed by deleting the corresponding directory; to release a device binding, contact nandflashtracer@gmail.com.

(e) How the default setting for the automatic installation of security updates required by Annex I, Part I, point (2)(c) can be turned off

See point (c) 5 of this item A.8. No automatic update function is configured.

(f) Information for integrators

107. NFT is a stand-alone desktop application intended for end users. The manufacturer provides **no SDK, library, plug-in interface or redistribution licence**, and the product is not designed to be integrated into other products in the form of a component;
108. Where you introduce the output of this product (reconstructed images, exported standard image files) into another forensic or recovery system, you, as the manufacturer or integrator of that system, must assess and fulfil the essential requirements of Annex I and the documentation requirements of Annex VII for that overall system yourself;
109. To facilitate that assessment, the manufacturer can provide on request: the list of supported input/output formats, the list of external interfaces and network

interactions (see section 3.3 of this document), an SPDX-format SBOM (see A.9) and an index to the documentation set listed in section 1.7;

110. Any natural or legal person that makes a **substantial modification** to NFT and places it on the market is, pursuant to Article 22 of the CRA, considered to be the manufacturer of that product in respect of the parts affected by the modification and must itself discharge the obligations under Articles 13 and 14.

A.9 Where the SBOM can be obtained (Annex II, point 9)

The manufacturer **does not publish the SBOM by default**. The SBOM is drawn up in SPDX 2.3 (JSON) format and covers at least the top-level dependencies of the product; it is provided upon a reasoned request from a market surveillance authority. Commercial users and integrators may also submit a request to nandflashtracer@gmail.com, and the manufacturer will provide the SBOM after verifying the identity of the requester.

Local data server.

Appendix B Mapping table for Annex I, Part I, point (2) and Part II

Applicability: applicable / partially applicable / not applicable. Where a requirement is determined to be "partially applicable" or "not applicable", the justification is recorded in CRA-RA-001 and, pursuant to Article 13(4), an explicit explanation is included in the technical documentation.

B.1 Annex I, Part I, point (2) (points (a) to (m))

Point	Essential requirement (summary)	Applicability	Measures implemented	Supporting evidence	Conclusion
(a)	Placed on the market without known exploitable vulnerabilities	Applicable	SBOM maintained; dependencies scanned for known vulnerabilities before release; fuzz and regression testing of the import parsing path; item-by-item confirmation in the pre-release security gate	CRA-SBOM-001, CRA-TR-001, CRA-VHP-001	Conformity
(b)	Placed on the market with a secure default configuration, including the possibility to	Applicable	Data processing is not networked by default; no telemetry; existing files not overwritten; output directory	Section 3.4, Appendix A.8(a)	Conformity

	reset the product to its original state		specified by the user; restoration of default settings and reinstallation provided as means of reset		
(c)	Vulnerabilities can be handled through security updates, including, where applicable, automatic security updates enabled by default, notification of available updates and the option to postpone	Partially applicable	Security updates and update notifications are provided; updates are released as separate patch-level versions and installation can be postponed; **the default state of the automatic security update switch and the means of turning it off are to be confirmed**	CRA-SUP-001, CRA-VHP-001; Appendix A.8(c)	Conditional conformity; to be re-assessed once placeholder P16 in section 13 is closed
(d)	Protection against unauthorised access through appropriate control mechanisms, and reporting of possible unauthorised access	Partially applicable	No multi-user account model and no network service; access control is implemented at the level of the operating system account and file system permissions; licence activation and device binding verification prevent the licence from being copied to unauthorised devices	Sections 3.1 and 3.3; CRA-RA-001	Partially applicable; justification set out in CRA-RA-001 (Article 13(4))
(e)	Protection of the confidentiality of data stored, transmitted or processed	Partially applicable	Data are processed locally and are not retained; HTTPS transport encryption is used for activation and updates;	Section 3.4, Appendix A.4 and A.8(a)	Partially applicable; justification set out in CRA-RA-001

			encryption at rest is provided by the operating system, and configuration guidance is given in Appendix A.4		
(f)	Protection of data, commands, programs and configuration against unauthorised manipulation, and reporting of corruption	Applicable	Imported images are checked for structure and checksum status, with corruption reported; project file structure is validated; update packages are checked for integrity and origin, with a version monotonicity check	Sections 3.2 and 4.3; CRA-TR-001	Conformity
(g)	Processing only of data that are adequate, relevant and limited to what is necessary (data minimisation)	Applicable	Only files explicitly selected by the user are read; no telemetry and no collection of personal data; activation transmits licence and device identifier fields only	Section 3.4; interface table in section 3.3	Conformity
(h)	Protection of the availability of necessary and basic functions, including resilience against and mitigation of denial-of-service attacks	Partially applicable	No external service and therefore no network DoS exposure; against local resource exhaustion, input size limits are applied, long-running tasks can be cancelled, and job state is persisted so that jobs can be resumed	Section 3.3; CRA-RA-001	Partially applicable; justification set out in CRA-RA-001

(i)	Minimisation of negative impact on the availability of services provided by other devices or networks	Applicable	No inbound listening port; does not reside as a service; no network scanning or broadcast behaviour; only outbound HTTPS connections perceptible to the user	Section 3.3	Conformity
(j)	Limitation of the attack surface, including external interfaces, in design, development and production	Applicable	The attack surface has been inventoried; the import path applies format allow-listing, structure validation, bounds checking and size limits; user-defined formulas use a restricted evaluator	Section 3.3; CRA-TR-001	Conformity
(k)	Reduction of the impact of an incident through appropriate exploitation mitigation mechanisms and techniques	Partially applicable	Runs with least privilege; does not reside as a service; no unsafe dynamic loading paths are used; **the configuration of compiler-level binary mitigations is to be confirmed**	Section 5.1; placeholder P06 in section 13	Conditional conformity; to be re-assessed once P06 is closed
(l)	Provision of security-related information by recording and monitoring relevant internal activity, with an opt-out for users	Partially applicable	A local job log is generated (containing no personal data) to support traceability; no centralised security monitoring or alerting is established, as this would exceed what is executable for a micro/small	Section 3.2; CRA-RA-001	Partially applicable; justification set out in CRA-RA-001

			enterprise; a log level setting is provided to disable or reduce logging		
(m)	Enabling users to securely and easily permanently remove all data and settings, and ensuring secure transfer of data where it can be transferred	Partially applicable	Uninstallation and manual deletion instructions are provided; output results are exported in standard image format to facilitate transfer; **the uninstaller, the default location of user data and the implementation status of a "clear user data" function are to be confirmed**	Appendix A.8(d); placeholder P15 in section 13	Conditional conformity; to be re-assessed once P15 is closed

B.2 Annex I, Part II (points (1) to (8))

Point	Requirement (summary)	Applicability	Measures implemented	Supporting evidence	Conclusion
(1)	Identify and document vulnerabilities and components, including an SBOM in a commonly used, machine-readable format covering at least the top-level dependencies	Applicable	SBOM in SPDX 2.3 (JSON) covering the top-level dependencies, updated before each release	CRA-SBOM-001	Conformity
(2)	Handle and remediate vulnerabilities without delay; provide security updates separately from functionality updates where	Applicable	Remediation deadlines set according to CVSS severity; security fixes are released as separate patch-level versions; where separation is not possible, the reason is stated in the advisory	CRA-VHP-001, CRA-SUP-001	Conformity

	technically feasible				
(3)	Effective and regular testing and review of the security of the product	Applicable	Security testing and review at least once every 12 months, with additional testing before major releases; exercises of the processes	CRA-TR-001	Conformity (execution dates and conclusions to be confirmed once placeholder P09 in section 13 is closed)
(4)	Sharing and public disclosure of information about fixed vulnerabilities after a security update	Applicable	Published on the website notice board and the forum, stating the description, affected versions, impact, severity and remediation guidance; disclosure is delayed only where the public risk outweighs the security benefit	CRA-CVD-001, CRA-SUP-001	Conformity
(5)	Establishment and implementation of a coordinated vulnerability disclosure policy	Applicable	A CVD policy has been drawn up and published, specifying the reporting channel, response deadlines, disclosure sequencing and the commitment not to pursue action against good-faith reporters	CRA-CVD-001	Conformity
(6)	Facilitating the sharing of information about potential vulnerabilities, including providing a contact address for reporting vulnerabilities	Applicable	nandflashtracer@gmail.com serves as the single point of contact and is included in Appendix A.2	Section 4.2, Appendix A.2	Conformity (evidence of publication to be confirmed once placeholder P01 in section 13 is closed)
(7)	Provision of mechanisms for the secure distribution of updates	Applicable	Restriction to official channels, HTTPS transport, SHA-256 checksum, version monotonicity check; code signing to be confirmed	Sections 4.3 and 5.6; CRA-SUP-001	Conditional conformity; to be re-assessed once P03 is closed
(8)	Release of security updates without delay and free of charge once available, accompanied	Applicable	Security updates are provided free of charge; an advisory is published with each release and known affected users are informed	CRA-SUP-001, CRA-VHP-001	Conformity

	by an advisory informing users				

13. Items pending confirmation (consolidated list of placeholders)

No.	Placeholder	Section(s)	Owner / note
P01	https://www.flash-tracer.com/about.html	4.2; Appendix B.2, point (6)	The "evidence of the contact address provided for reporting vulnerabilities" required by Annex VII, point 2(b)
P02	https://www.flash-tracer.com/about.html	5.5	Needed to describe the distribution channel and transport protection for security updates
P03	Provide MD5 value for integrity verification.	4.3, 5.6; Appendix B.2, point (7)	Affects the conclusions for points (c), (f) and (k) of Part I
P04	internal build identifier Ver 2.26.8.26 2.26.8.26-20260826	2.1, Appendix A.3	Element allowing identification of the product under Article 13(15)
P05	The source-code version-control server is not connected to external networks, and passwords are known only to a minimum scope of personnel.	5.2	Element of verification of the production and monitoring processes
P06	VS2022	5.1; Appendix B.1, point (k)	Affects the conclusion for point (k) of Part I
P07	https://www.flash-tracer.com/ The form contains only the activation code.	3.3	Needed to describe the only network interaction and data minimisation
P08	Release packages are stored on a local data-backup server which is not connected to the network. Each version is backed up, and the server performs monthly backups.	5.7	Retention of evidence of continued conformity under Article 13(14)
P09	Test completion date: August 24, 2026.	8; Appendix B.2, point (3)	Required by Annex VII, point 6

	Test result: Passed.		
P10	Finalization date: September 3, 2026. Evaluation result: No risk.	9	Required by Annex VII, point 3
P11	September 3, 2026. https://www.flash-tracer.com/about.html	10, Appendix A.6	Annex II, point 6; Article 13(20)
P12	September 3, 2026. https://www.flash-tracer.com/about.html	11, Appendix A.9	Annex VII, point 8
P13	February 10, 2024	12.2	Determines the actual retention deadline for the technical documentation
P14	Stored on a local data-backup server which is not connected to the network. Each version is backed up, and the server performs monthly backups.	12.5	Ability to make documentation available under Article 13(13) and (22)
P15	Uninstallation only requires deleting the program folder; no files exist in other locations.	Appendix A.8(d); Appendix B.1, point (m)	Affects the conclusion for point (m) of Part I
P16	No automatic update function is configured.	4.3; Appendix A.8(c) and (e); Appendix B.1, point (c)	Affects the conclusion for point (c) of Part I; required by Annex II, point 8(e)
P17	A prompt will be shown upon software startup after license expiration.	6.4	Second sentence of Article 13(19)
P18	This shall be stated in the contract.	6.3	First sentence of Article 13(19)

*Note: Each placeholder above will be replaced with the actual content once the corresponding matter is confirmed, and the affected compliance conclusions will be updated accordingly (see the "Conclusion" column of Appendix B). Until a placeholder is closed, the corresponding conclusion in this document is one of **conditional conformity** and does not constitute a basis for the final statement of conformity.*

Signature record

Role	Name	Signature	Date
Prepared by	Jin Cancan		2 September 2026
Reviewed by	Zhou Yang		2 September 2026

Approved by	Zhou Yang		2 September 2026