EXPUNGEDATA

Certificate of Data Sanitization

Certificate ID: SSR-2025-SAMPLE-EXP1

Date Issued: December 18, 2025

NIST 800-88r2 | IEEE 2883 | ISO 27040

ORGANIZATION
CUST-GIP-021

CONTACT
Sarah Chen

IDENTITY

IDENTIFICATION

Serial Number
S5HRNG0R901234

Manufacturer
Samsung

Model
Samsung SSD 870 EVO 1TB

Firmware
SVT04B6Q

SPECIFICATIONS

Capacity
931.51 GB

Interface
SATA III

Drive Type
SSD

Form Factor
2.5"

SANITIZATION RECORD

Method
ATA Secure Erase

Started
2025-12-18 15:25:00 UTC

Completed
2025-12-18 15:26:30 UTC

Tool
sedutil 1.20.0

Duration
1m 30s

Verification
Block Inspection

Result
✔ **PASS**

DRIVE CONDITION SUMMARY

Health Grade
A

SMART Status
PASSED

Life Remaining
97%

Power-On Hours
4,380

Power Cycles
42

Temperature
32°C

Critical SMART Errors
None

Total Data Written
21.97 TB

Reallocated Sectors
0

Pending Sectors
0

Offline Uncorrectable
0

METHODOLOGY

Data sanitization was performed in accordance with the following standards and guidelines: NIST Special Publication 800-88 Revision 2: Guidelines for Media Sanitization; IEEE 2883-2022: Standard for Sanitizing Storage; ISO/IEC 27040:2024: Storage Security. The sanitization process applied the Clear method to all media listed in this certificate. Pattern-based overwrite with read-back verification was performed on each device to confirm successful data removal. Hidden areas (HPA/DCO) were checked and addressed where applicable per NIST SP 800-88r2.

VERIFICATION

Verified via block inspection Tool: sedutil v1.20.0.

NIST SP 800-88 REV. 2 COMPLIANCE

Media Type: ISM

Sanitization performed in accordance with IEEE 2883-2022 and NIST SP 800-88r2 (September 2025).

CHAIN OF CUSTODY

DATE RECEIVED	LOCATION	TECHNICIAN
December 18, 2025	Expunge Data Services, Southlake, TX	Automated

ATTESTATION

I attest that the storage devices described in this report were sanitized in accordance with the methodology stated above. Each device was verified per our standard process. This Sanitization Service Report is an accurate record of the sanitization services performed. This report is self-attested documentation and has not been independently certified by any third-party accrediting body.

PERSON PERFORMING SANITIZATION

Electronically attested by Jordan Reyes

Name / Title: Jordan Reyes / Senior Sanitization Technician

Organization: SecureMedia Services LLC

Location: Plano, TX 75024

Phone: (469) 555-0142 Email: j.reyes@example.com

Date: December 18, 2025

CONCURRENCE

Signature

Name / Title: _____

Organization: _____

Location: _____

Phone: _____ Email: _____

Date: _____

CERTIFICATE VERIFICATION

Verify this certificate:

https://expungedata.com/verify/SSR-2025-SAMPLE-EXP1?drive=S5HRNG0R901234

Document Hash (SHA-256):

fd6cdd1458ef054e98bde35f7d52caeb972dd9148b17f834342fd7304dcab934

IMPORTANT DISCLAIMERS

This Sanitization Service Report documents the data sanitization process performed by ExpungeData, a service of FitzgeraldTech LLC ("Provider"), on the media identified above.

SCOPE OF THIS REPORT

This report attests that the specified sanitization method was applied to the identified media using the documented tools and processes. This report does NOT constitute a guarantee, warranty, or insurance against data recovery by any means. This report does not attest to the content, classification, regulatory status, or value of any data that may have been present on the media.

NO CERTIFICATION CLAIM

ExpungeData's sanitization processes are aligned with the guidelines published in NIST Special Publication 800-88 Revision 2 (September 2025) and IEEE 2883-2022. This alignment is self-attested and has not been independently verified or certified by NIST, IEEE, any government agency, or any accrediting body. References to NIST SP 800-88 and IEEE 2883 indicate alignment with published guidelines, not certification.

LIMITATIONS OF SOFTWARE-BASED SANITIZATION

Software-based sanitization (Clear and Purge methods) operates through the media's standard logical interface. Provider cannot guarantee sanitization of data stored in areas inaccessible to the logical interface, including but not limited to: firmware regions, Host Protected Areas (HPA), Device Configuration Overlays (DCO), remapped or reallocated sectors, wear-leveled blocks on flash-based storage, or physically damaged sectors. For maximum sanitization assurance, the Destroy method is recommended.

CLIENT RESPONSIBILITY

The client is solely responsible for determining regulatory, legal, and contractual requirements applicable to the destruction of their data, including requirements under HIPAA, PCI DSS, SOX, GLBA, FACTA, GDPR, CCPA, TDPSA, and any other applicable law. Provider does not provide legal, regulatory, or compliance advisory services. This report may not satisfy all regulatory documentation requirements. Clients should consult qualified legal counsel to determine whether this report meets their specific compliance obligations.

RETENTION

Provider retains a copy of this report and associated chain of custody records for a minimum of seven (7) years from the date of issuance. Client is responsible for maintaining its own copies.

GOVERNING TERMS

This report is subject to the Terms of Service agreed to by client. In the event of any conflict, the Terms of Service shall govern.