CONNECT new mexico
Office of Broadband Access & Expansion

Frequently Asked Questions

SECURE DATA DESTRUCTION

DIGITUNITY

© 2025 DIGITUNITY. ALL RIGHTS RESERVED.

Secure Data Destruction FAQs

Media sanitization is a core competency for corporate information technology departments and IT asset disposition firms in the context of data privacy, data security, and regulatory compliance. Growing concerns about data privacy along with media proliferation has turned data sanitization into a critical business need.

Data erasure software is an essential tool that ensures data security at the end of the asset life by completely removing sensitive information by purposely, permanently deleting, or destroying data from a storage device, to ensure it cannot be recovered.

There are various information destruction standards today, each with specific methods and guidelines, to serve the company's media sanitization needs. The National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce developed the NIST Cybersecurity Framework to help businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. For instance, NIST Special Publication 800-88, laid down under the Federal Information Security Management Act of 2002, outlines Clear, Purge, and Physical Destruction as the 3 recommended methods for media sanitization.

NIST Clear and NIST Purge are the preferred methods for sanitizing media (wherever feasible and sufficient). That's because both Clear and Purge methods rely on logical techniques – overwrite, block erase, and cryptographic erase – to sanitize the media. This is beneficial because there is no e-waste generation and the storage media can be reused.

© 2025 DIGITUNITY. ALL RIGHTS RESERVED.

FREQUENTLY ASKED QUESTIONS:

What is NIST SP 800 88 standard?
NIST has issued an updated version of Special Publication (SP) 800-88 guidelines for Media Sanitization. The NIST data erasure standard is a secure erase method that can be used to sanitize a vast variety of media including ATA hard disk drives and Solid State Drives (SSDs), mobile devices, USB removable media, optical media, etc.

How secure is the NIST 800-88 standard?
NIST 800-88 is extremely secure and defines the safest methods of IT assets disposition. Laid down under the Federal Information Security Management Act of 2002, the NIST SP 800-88 standard suggests Clear, Purge, and Physical Destruction as the top three media sanitization approaches.

What is NIST Clear?
The NIST Clear method uses standard read/write commands, techniques and tools to overwrite all the user-addressable locations including logical file storage locations on an ATA hard drive or SSD with non-sensitive data (binary 1s and 0s).

What is NIST Purge?
The NIST Purge method involves Overwrite, Block Erase, and Cryptographic Erase as the logical techniques for sanitizing ATA hard disk drives and SSDs. The Purge method uses the overwrite EXT command to overwrite – i.e. apply a single write pass of a fixed pattern (all 0s or a pseudorandom pattern) – on ATA hard disk drives. Optionally, it may apply three total write passes of a pseudorandom pattern so that the second write pass is the inverted version of the original pattern.

Can You Wipe SSD Using NIST 800-88?
Yes, NIST 800-88 advocates using Clear and Purge techniques to securely perform data wiping on SSDs.

© 2025 DIGITUNITY. ALL RIGHTS RESERVED.

ADDITIONAL INFORMATION AND RESOURCES

The following section outlines the specific techniques and additional details within NIST Data Erasure Standard:

NIST Clear techniques for erasing hard disk drives and SSDs:
TThe NIST Clear method uses standard read/write commands, techniques and tools to overwrite all the user-addressable locations including logical file storage locations on an ATA hard drive or SSD with non-sensitive data (binary 1s and 0s).

The Clear pattern for media overwriting should include at least a single write pass with a fixed data value such as all zeros. Multiple write passes or values that are more complex may optionally be used.

Note: Overwriting on SSDs (flash storage) may reduce the effective lifetime of the media. Also, it may not sanitize the data in unmapped physical media.

NIST Purge techniques for erasing hard disk drives and SSDs:
The NIST Purge method involves Overwrite, Block Erase, and Cryptographic Erase as the logical techniques for sanitizing ATA hard disk drives and SSDs.

- The Purge method uses the overwrite EXT command to overwrite – i.e. apply a single write pass of a fixed pattern (all 0s or a pseudorandom pattern) – on ATA hard disk drives. Optionally, it may apply three total write passes of a pseudorandom pattern so that the second write pass is the inverted version of the original pattern.

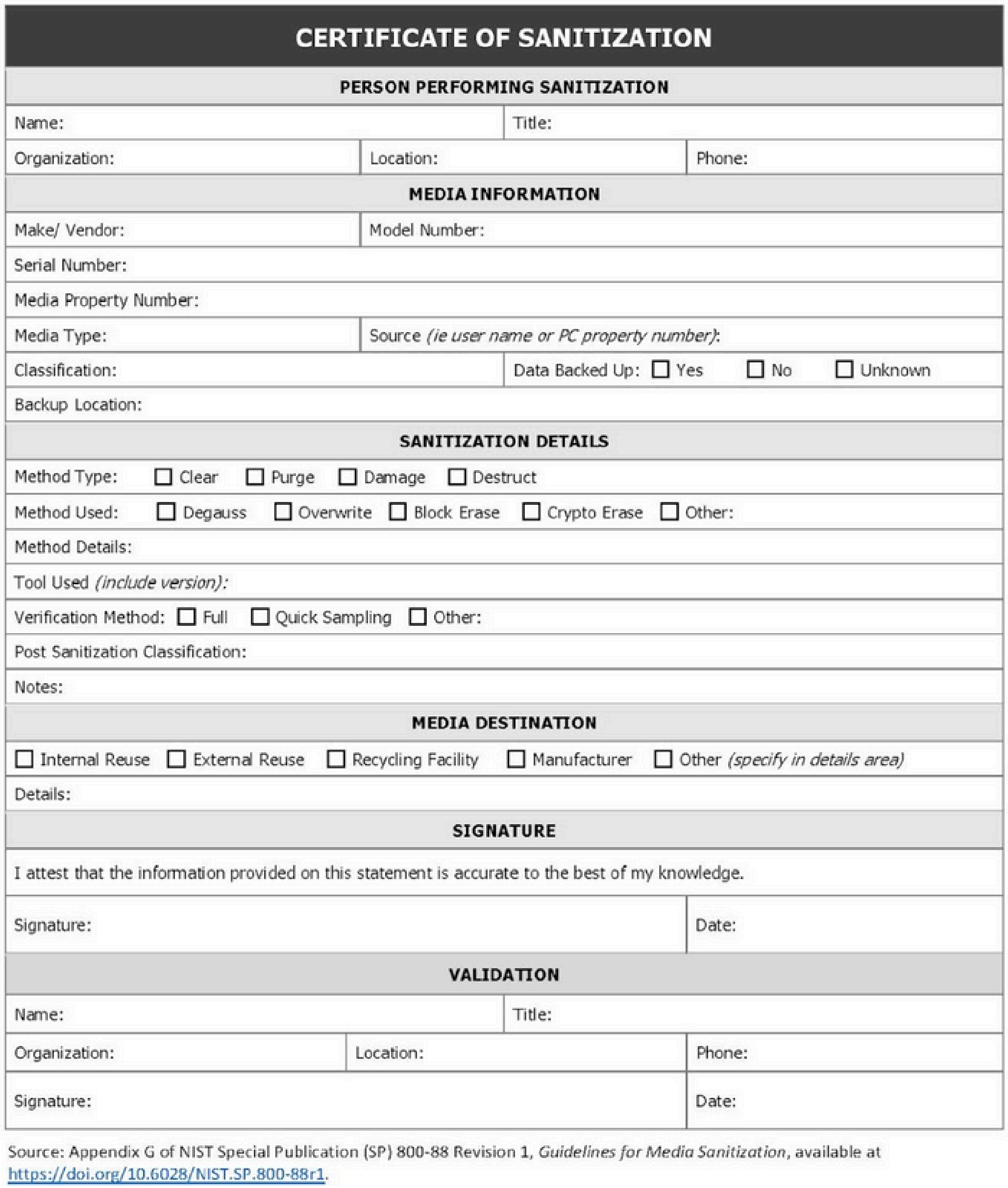
© 2025 DIGITUNITY. ALL RIGHTS RESERVED.

- Block Erase is the secondary erasure method for SSDs, which "electrically" erases each block by using internal SSD functions. After successful implementation of the block erase command, the method applies binary 1s across all the user-addressable locations on the storage media and then repeats Block Erase.

- NIST Purge also specifies use of Cryptographic Erase command to sanitize ATA hard drives and SSDs that support encryption. Cryptographic Erase can be optionally accompanied with single-pass Overwrite, Secure Erase or Clear techniques, based on the media support.

© 2025 DIGITUNITY. ALL RIGHTS RESERVED.

Sample Certificate of Destruction/Sanitization



CERTIFICATE OF SANITIZATION

PERSON PERFORMING SANITIZATION

Name: | Title:

Organization: | Location: | Phone:

MEDIA INFORMATION

Make/ Vendor: | Model Number:

Serial Number:

Media Property Number:

Media Type: | Source *(ie user name or PC property number)*:

Classification: | Data Backed Up: □ Yes □ No □ Unknown

Backup Location:

SANITIZATION DETAILS

Method Type: □ Clear □ Purge □ Damage □ Destruct

Method Used: □ Degauss □ Overwrite □ Block Erase □ Crypto Erase □ Other:

Method Details:

Tool Used *(include version)*:

Verification Method: □ Full □ Quick Sampling □ Other:

Post Sanitization Classification:

Notes:

MEDIA DESTINATION

□ Internal Reuse □ External Reuse □ Recycling Facility □ Manufacturer □ Other *(specify in details area)*

Details:

SIGNATURE

I attest that the information provided on this statement is accurate to the best of my knowledge.

Signature: | Date:

VALIDATION

Name: | Title:

Organization: | Location: | Phone:

Signature: | Date:

Source: Appendix G of NIST Special Publication (SP) 800-88 Revision 1, *Guidelines for Media Sanitization*, available at https://doi.org/10.6028/NIST.SP.800-88r1.

© 2025 DIGITUNITY. ALL RIGHTS RESERVED.