ZeroData™ Windows® Storage Drive Eraser

Only 1-tool required…. ZeroData™Windows® meets all data erasure requirements, regardless of drive type… defeat sophisticated software or hardware recovery tools… wipe data permanently… Complies to GDPR, government, military, NIST and ISO/IEC standards…

Reliable, total data cleaning is what ZeroData™ Windows® solves. Permanently and safely remove all data, regardless of drive type, conforming to data destruction levels specified by major organisations and government bodies for PC reassignment, upgrades, refurbishment, recycling.

ZeroData Windows advantages are simple — determine drive integrity, or not — fast and cost effective data wiping for all types of hard drives, plus **separate erasure protocols for Solid State Drives, ATA firmware erasure, Purge erase NVMe disks connected to iRST and RAID systems** too. Diverse, yet easy to use, select compliance standards to meet different erasure criteria. Prepares PDF validation certificates and saved reports for confirmation — proof — of potentially sensitive data removal. **Trust ZeroData Windows for proof of permanent erasure** demanded by compliance standards. Since 2002, ZeroData has ensured customer confidence with 100% data erasure. **No over-managed file administration — just secure, reliable, data wiping results.**

Powerful, easy-to-use data erasure	✔ *Options to meet or exceed data destruction levels specified by major organizations and Government bodies. Including current NIST 800-88 Rev.1 & ISO/IEC 27040:2015 methods.*
Multiple security level options available	✔ *Overwrite the master boot record, hidden partition, and locked areas regardless of BIOS restrictions using multiple passes.*
Runs in bootable Windows® operating system. Integrates Eurosoft Diagnostics	✔ *Compatible with Windows® 7, 8x, 10 operating systems. Including Windows PE for pre-boot operation or command line automation for industry scaling. Integrates with PC Builder™ and Pc-Check Windows.*
Erase up to 99 hard drives in parallel and simultaneously, regardless of type	✔ *For RAID, SCSI, SATA, SAS, SSD, NVMe, IDE, and removable storage devices.*
ATA/SCSI/SAS/NVMe firmware erasure methods with added verification	✔ *Wipe data in minutes not hours. Use hard disk inbuilt erasure commands and confirm data erasure on completion.*
Digitally signed detailed, full data erasure very secure reporting	✔ *Tamper proof digital report signature provides secure audit trail Printable Text and PDF validation reports or XML logs that include user and PC identification.*
Industry first – create 12N Smart Labels conforming to ANSI/MH10 Standards	✔ *Store detailed information with 4000 characters instead of 500, in a single label. Maintain your audit trail with 12N Smart labels.*

Trust ZeroData™ Windows erasure software… no sector left behind… Millions of drives securely erased… *Now you can relax*.

ZeroData™ Windows® Software

Erase up to 99 physical drives at once, and in parallel across hard and SSD drives, USB.

License by how many systems' drives you want to erase. In parallel at one-time.

Runs in 32-bit and 64-bit Windows® operating systems, WinPE (auto-boot) and command line industry scale too.

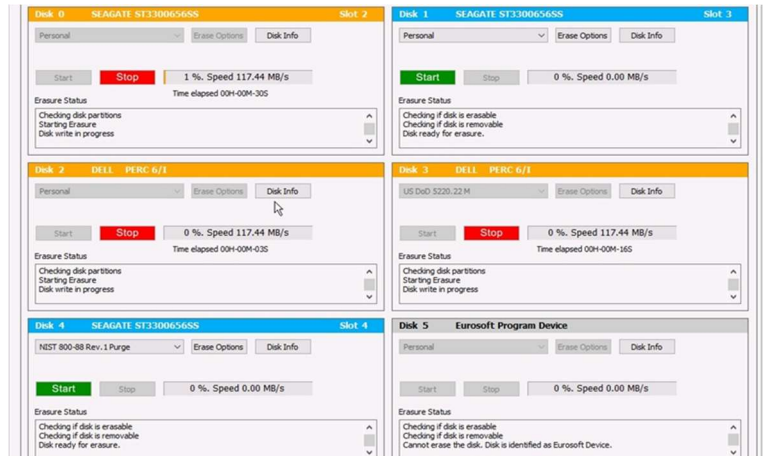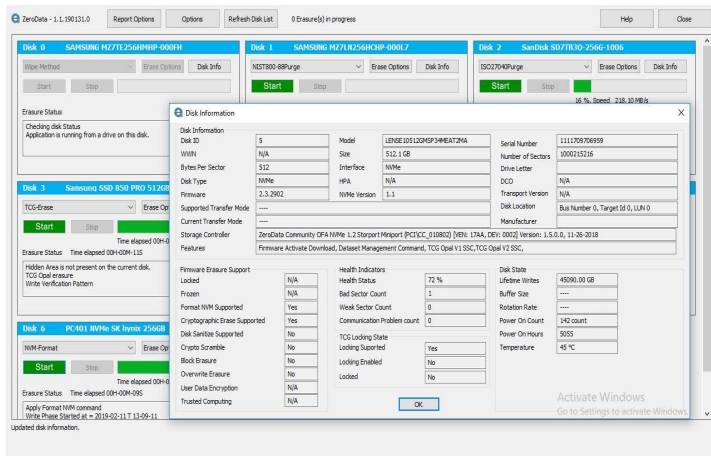Multiple industry standard and government compliant erasure methods to choose from.

ATA Firmware erasure methods and added verification.

Fastest, specific erasure methods for SSD's.

Windows driver availability enhances RAID erasure options.

Drive Initialise option for operating system deployment.

Industry standard XML reports align with Eurosoft Pc-Check® Diagnostic & PC Builder™ software family.

ZeroData™ Windows® helps you...

• Conveniently and safely remove sensitive or unwanted information from PC physical drives, ATA/SSD.

• Confidently refurbish, upgrade, recycle, donate, and return leased PCs.

• Comply with your choice of data removal standards.

• Provide an audit trail for reassigned equipment.

• Contributes data to regulations such as WEEE, SERI R2, HIPA, ADISA, GDPR and NAID.

Overwrite the master boot record...hidden partitions...locked areas... regardless of BIOS restrictions

• Statistically secure random passes.

• Block sophisticated data recovery techniques.

• Unique non-linear pass option.

• Erases any drive… up to 99 drives in parallel and simultaneously with choice of license type.

• For RAID, SATA, SAS SCSI, SSD, IDE, NVMe, USB and removable storage devices.

• Network delivery options available. Windows PE version for use with PC Builder; provides automated drive erasure.

• Initiate ATA firmware erasure methods. Remove data in minutes not hours. With added verification to confirm successful data erasure.

• Identify and erase drives connected by Intel Rapid Storage Technology. No need to disable iRST and reboot. Even perform Purge erase on NVMe drives connected to iRST.

• Erases drives of 2 Terabyte capacity or more. Lower capacity too.

Ensure the drive is completely clean...data cannot be retrieved

• Printable PDF validation certificates.

• Tamper proof reports include user and PC identification.

• Erasure logs record methods, how many passes were made, and more.

• Presents erasure dates and times, sector errors, and more.

• Option to finish with a 'zeroing pass' to prepare for a clean, new operating system install.

• Option to execute additional erasure passes in addition to the selected erasure method. Up to 99 extra zero, random or nonlinear passes each.

• Erase all disks confidently while excluding specific drives or all removable disks including USB disks and memory cards from erasure.

• Print labels that can be applied to drive surface or protective bags.

ZeroData™ Windows® reports Disk Health Status

• Reflect the SMART status of drives before and after using ZeroData Windows.

• Obtain SMART data – such as hard disk temperature –from ATA-type drives.

ZeroData Disk Erasure Certificate
Eurosoft (UK) Ltd

Licensee Name: **Development**
Operator Name: **ГÇ£Johnny AppleseedГÇ¥**   Supervisor Name: **ГÇ£Jason WhiteГÇ¥**
Log UUID: **262eb2ba-1f9b-4131-a89b-78ebcfe844e0**
Data Erasure Software Used: **ZeroData ver. 1.6.1.0305 built on: 2021-03-05**

Erasure Operation Details   Passed: 0 Failed: 1

Disk: 1 Information

Vendor: **N/A**	Model: **WDC WDS120G2G0A-00JH30**	Nominal Size: **120.0 GB**
Disk Type: **SSD**	Serial Number: **180873800087**	WWN: **5001B448B6BF6186**
Size: **111.8 GB**	Sector Size: **512**	Sectors: **234455040**
HPA: **Not Present**	DCO: **N/A**	Interface: **S-ATA Gen3, 6 Gbps**
Power On Count:	Power On Hours:	Total Host Writes:
Reallocated Sectors Before: **0**	Uncorrectable Sectors Before: **0**	Current Pending Sectors Before: **0**
Reallocated Sectors After:	Uncorrectable Sectors After:	Current Pending Sectors After:
Bad Sectors Before Erasure: **0**	Bad Sectors After Erasure:	Health Status: **79 %**
Health Status After Erasure:	Storage Controller: **Intel(R) Chipset SATA/PCIe RST Premium Controller (RAID)** [VEN: 8086, DEV: 2822] Version: 17.9.1.1009, 6-2-2020	

Erasure Operation

Status: **Failed**		Failed Count: **79**
Erasure Passes: **0**	Verify Passes: **0**	Fingerprint Written:
Started At: **2021-03-09 08-26-14**	Ended At: **2021-03-09 08-26-14**	Total Duration: **00H-00M-00S**
Erasure Method: **Check SMART Data**	Method: **Health Status Percentage**	
Method Used:	Extra Methods: **N/A**	

Ⓧ Disk health status below threshold. Please destroy disk. Health: 79 %

Erasure System Hardware Details

Manufacturer: **To Be Filled By O.E.M.**	Product Name: **To Be Filled By O.E.M.**	Version: **To Be Filled By O.E.M.**
Serial Number: **To Be Filled By O.E.M.**	UUID: **A3C28570-AEFE-0000-0000-000000000000**	SKU: **To Be Filled By O.E.M.**

BaseBoard: **ASRock, Z390 Pro4, NULL, M80-B8007504808, NULL**
Processor: **CPU0, Central Processor, BFEBFBFF000906EC, Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, Core: Intel64 Family 6 Model 158 Stepping 12**
BIOS Details: **American Megatrends Inc., Version: P4.30, Date: 08/12/2019**
Installed Memory: **8 GB**
OS Details: **Version: Windows (TM) 10 Preinstallation Environment [6.3], ServicePack : 0.0, 64Bit: True**
UEFI Enabled: **True**

Report Details

Report UUID: **a03770a0-c187-42a5-b326-e54ef9096607**
Report Date: **2021-03-09 08-25-12**
Software Used: **ZeroData ver. 1.6.1.0305 built on: 2021-03-05**
Digital Signature: **wbqpEXMDtaN651in9QI//cEyIARS5QqzJAHIj7BpGjZDhN01Js4BqEGw5UD7Fd9fjIKcJNiGwld97Baoy+k7mTs64IXL8wPGZaaHdts5 WQsYW/pMeb/rx13SFq1KN6ZCdhcKYhyb4RyndCoHjuWaaw/e+Rs7ay9F/G8x3BcgnPZFViJatTZln2jdIT7keL88GD7WEOYaxOIYFy zEbEH4ukmry3G7Hp1ydojpl9WToClR1YvDlNO9/E24PA0BpHpv**

I hereby state that the data erasure process has been carried out in accordance with the given instructions.

_____   _____
Data Erasure Operator   Data Erasure Supervisor

Model	ST1000DM003-1ER162
SN	W4Y1V7T6
Capacity	1.0 TB Health **100 %**
Status	SUCCESSFUL Method NIST800-88PURGE
Bootable	NO Time 2020-04-24 10-08-18

ZeroData™ Windows® report options. Providing the What? Who? Where? And When?

- Uniquely identify all erased disks.
- Identify the operator, customer, location and time.
- Proof that the selected data erasure method and status meets the required criteria.
- Identify the number of bad blocks and disk health status to determine reuse or disposal.
- Record of system hardware details, including drive health for continued performance.

Trusted, tamper proof, digitally signed PDF erasure certificate — a secure audit trail for logistical information of reassigned and redistributed equipment.

Feature	ZeroData Windows
SSD Erasure	✓
RAID Erasure	✓
Removable Storage Devices	✓
NIST SP 800-88Clear	✓
NIST SP 800-88Purge	✓
ISO/IEC 27040:2015 Clear	✓
ISO/IEC 27040:2015 Purge	✓
ATA-Secure Erase	✓
ATA-Enhanced Secure Erase	✓
ATA-Sanitize	✓
ATA-Crypto-Block Erase	✓
SCSI-Sanitize	✓
SCSI-Format Unit	✓
Sanitize-Overwrite	✓
Sanitize-Crypto	✓
Sanitize-Block	✓
NVM-Format	✓
TCG-Erase	✓
Eurosoft SSD Standard	✓
Eurosoft SSD Random4	✓
Eurosoft SSD Random6	✓
HMGIS5Higher	✓
HMGIS5Lower	✓
Eurosoft Personal	✓
Eurosoft Professional	✓
Eurosoft Corporate	✓
Eurosoft Military	✓
Eurosoft Fast	✓
Eurosoft Standard	✓
Eurosoft Deep	✓
Drive Initialize	✓
Gutmann	✓
US DoD-M	✓
Bruce Schneier	✓
NAVSO P-5239	✓
NCSC-TG-025	✓
Air Force 5020	✓
US Army AR380-19	✓
German VSITR	✓
RCMP TSSIT OPS-II	✓
CSEC ITSG-06	✓
OPNAVINST	✓
NSA 130-1	✓
US DoD-M-ECE	✓
German SI-2011-VS BSI-GS	✓
German SI-2011-VS BSI-GSE	✓
Text, PDF or XML Erasure Reports	✓
Tamper Proof Confirmation Reports	✓
Print & Attach Erasure Labels	✓

Note: Windows PE v1.x contains a security feature that will cause end user's systems to reboot without prior notification to the end user after 24 hours of continuous use. Windows PE v2.x contains a security feature that will cause end user's systems to reboot without prior notification to the end user after 72 hours of continuous use.

Eurosoft
computer reliability solutions