Blank is Compliant

Thank you for downloading this Blancco datasheet. Carahsoft is the reseller for Blancco Fed and Sled solutions available via GSA 2GIT, CMAS, GSA MAS, and other contract vehicles.

To learn how to take the next step toward acquiring Blancco's solutions, please check out the following resources and information:

For additional resources:
carah.io/BlanccoResources

For upcoming events:
carah.io/BlanccoEvents

For additional Riverbed solutions:
carah.io/BlanccoSolutions

For additional FED and SLED solutions:
carah.io/BlanccoSolutions

To set up a meeting:
Blancco@carahsoft.com
866-421-4683

To purchase, check out the contract vehicles available for procurement:
carah.io/BlanccoContracts

For more information, contact Carahsoft or our reseller partners:
Blancco@carahsoft.com | 866-421-4683

Blank is compliant

There are dozens of data wiping and erasure standards that may affect your organization. Whatever ones you use, you can rest assured that our software can handle them.

Modern organizations have diverse data storage capabilities and equally diverse compliance requirements for sanitizing that data.

Blank is complaint because it offers one solution to dozens of standards.

Compliance requirements for data management don't end when your IT assets are decommissioned.

There are numerous data erasure and data wiping standards for the secure removal of sensitive information from PC hard drives, removable media, LUNs, and other storage devices. Rigorous standards for these data sanitization procedures are set forth by government agencies and private organizations around the globe.

These standards dictate how that data is handled, even after assets are off your company network and no longer in active use.

Blank is compliant because it enables you to sanitize your data according to whichever standard best fits your organization's needs—and provides the certificate of erasure to prove it.

Decommissioning your IT? You'll need an erasure standard

Standards are set forth by government agencies and private institutions to ensure quality and consistency. Regarding data erasure, standards normally differ on the number of overwrites and what pattern is used to overwrite a data storage device.

The most well-known data sanitization standards or guidelines may be the 3 and 7-pass methods from the U.S. Department of Defense (DoD 5220.22-M/ECE) and the NIST SP 800-88, Rev. 1 Clear and Purge standards, but others may be more popular in various regions or industries.

The newest data sanitization version is IEEE 2883-2022 from the IEEE Standards Association.

This IEEE Standard for Sanitizing Storage "specifies methods of sanitizing logical storage and physical storage, as well as providing technology-specific requirements and guidance for the elimination of recorded data."

View the data wiping and erasure standards below, then decide which one(s) is the best fit for your business.

Standard Name	# of Passes	Description
Air Force System Security Instruction 5020	2	Originally defined by the United States Air Force, this 2-pass overwrite is completed by verifying the write.
Aperiodic random overwrite/Random	1	This process overwrites data with a random, instead of static, pattern. Each sector of the drive will contain different data. This process is completed by verifying the write.
Blancco SSD Erasure	Proprietary	Blancco's multi-phase, proprietary SSD erasure approach utilizes all supported SSD security protocols. This innovative method includes multiple random overwrites, firmware level erasure, freeze lock removal and full verification.
Bruce Schneier's Algorithm	7	This 7-step process, presented by security technologist Bruce Schneier, overwrites using 1s, 0s and a stream of random characters.
BSI-2011-VS	4	This 4-pass system is the original BSI standard defined by the German Federal Office of Information Security.

Standard Name	# of Passes	Description
BSI-GS	1	Defined by the German Federal Office for Information Security, this process begins by removing hidden drives (HPA/ DCO if existing) and overwriting with aperiodic random data. The next step triggers a firmware based command dependent on the type of drive. The last step is to verify the write.
BSI-GSE	2	The BSI-GSE adds one extra step to the BSI-GS. After the first overwrite, an additional overwrite with aperiodic random data is added before moving on to the last two steps.
CESG CPA – Higher Level	3	The UK government's National Technical Authority for Information Assurance standard is a 3-pass process with a verification after each step.
Cryptographic Erasure (Crypto Erase)	N/A	This method uses the native command to call a cryptographic erasure, which erases the encryption key. While the encrypted data remains on the storage device itself, it is effectively impossible to decrypt, rendering the data unrecoverable. Because this method uses the native commands as defined by the manufacturer, it is only available if supported by the drive being erased.
DoD 5220.22-M	3	Published by the U.S. Department of Defense (DoD) in the National Industrial Security Program Operating Manual (also known as DoD document #5220.22-M), it specified a process of overwriting hard disk drives (HDDs) with patterns of ones and zeros. The process required three secure overwriting passes and verification at the end of the final pass. More on this standard is available at our blog, "Everything You Need to Know About the DoD 5220.22-M Disk Wiping Standard & Its Applications Today".
DoD 5220.22-M ECE	7	This method is an extended (7-pass) version of the DoD 5220.22-M. It runs the DoD 5220.22-M twice, with an extra pass (DoD 5220.22-M (C) Standard) sandwiched in between.

Standard Name	# of Passes	Description
Extended Firmware Based Erasure	3	This Blancco-defined standard adds an overwrite as the first step and then follows the standard Firmware Based Erasure, making this a 3-step process.
Firmware Based Erasure	2	This Blancco-defined standard is a 2-step process triggers a firmware command that is dependent on the drive type. The last step of the process is to verify the write.
HMG Infosec Standard 5, Higher Standard	3	Used by the British Government, this 3-pass overwrite adds one additional write. Like the baseline standard, this process is completed by verifying the write.
HMG Infosec Standard 5, Lower Standard	1	Used by the British Government, this 1-pass overwrite consists of writing a zero pattern. This process is completed by verifying the write.
IEEE 2883-2022 Clear	0-2	Developed by the IEEE Standards Association, IEEE Clear requires the removal/erasure of certain areas (such as hidden areas, depopulated storage elements, or cache zones, if existing). The data is then sanitized (via a firmware-based command or overwritten) and verified. To learn more, see our article, "New IEEE Data Erasure Standard Fills Technology Gap"
IEEE 2883-2022 Purge	0-2	Developed by the IEEE Standards Association, IEEE Purge requires the removal/erasure of certain areas (such as hidden areas, depopulated storage elements, or cache zones, if existing). The data is then sanitized (via a firmware-based command) and verified. To learn more, see our article, "New IEEE Data Erasure Standard Fills Technology Gap"
National Computer Security Center (NCSC-TG-025)	3	Defined by the US National Security Agency, this 3-pass system includes a verification after each pass of 0s, 1s and a random character.
Navy Staff Office Publication (NAVSO P-5239-26)	3	Published by the US Navy, this 3-pass system uses a specified character (and its complement) and a random character. The process is completed by verifying the write.

Standard Name	# of Passes	Description
NIST 800-88 Clear	0-2	The National Institute of Standards and Technology Clear requires the removal of hidden areas (HPA/DCO, if existing). The data is then overwritten and verified.
NIST 800-88 Purge	0-2	This method requires the removal of hidden areas (HPA/DCO, if existing). A firmware-based command is triggered depending on the type of drive, and the last step is the verify the write. Our NIST Guide gives more detail.
NSA 130-1	3	Defined by the National Security Agency, this method uses a 3-pass overwrite: writes a random character, writes another random character and writes a known value. This process is completed by verifying the write.
OPNAVINST 5239.1A	3	Defined by the US Navy, this process is completed by verifying the write after a 3-pass overwrite—the first a random byte and static overwrite for the last two.

Need a specific data wiping and erasure standard? We've got you covered.

As the global leader in certified data erasure, Blancco supports 24+ international data wiping and erasure standards set by government agencies, legal authorities, and independent testing laboratories, including all the ones listed above.

Regardless of the internal standard(s) required by your government or organization, Blancco solutions can help you prove compliance and protect your data.

The Blancco Perspective

While standards and requirements will evolve with technology, **Blank is compliant** because it's consistent.

The latest IEEE 2883-2022 standards won't be the last, but they are the best for sustainably protecting data on newer decommissioned assets.

As new technologies continue to develop, we'll continue to develop new ways to fulfill the sanitization requirements enterprises follow to protect their data.

Stay Current on Compliance

Stay up to date on the latest data privacy requirements and regulatory changes that may affect your organization.

Visit our content hub