blancco

Blancco Erasure Standards

As the de facto global standard in certified data erasure, Blancco supports 25 international erasure standards set by government agencies, legal authorities and independent testing laboratories. Regardless of the internal standard(s) required by your government or organization, Blancco solutions can help you prove compliance and protect your data.

	Overwriting Rounds		BLANCCO DRIVE ERASER	BLANCCO MOBILE DEVICE ERASER	BLANCCO VIRTUAL MACHINE ERASER, LUN ERASER, FILE ERASER, BLANCCO REMOVABLE MEDIA
		TOTAL	22	15	16
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	Prop.*	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.	✖	✖	✓
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.	✓	✖	✓

continued...

*Prop. = Proprietary

			BLANCCO DRIVE ERASER	BLANCCO MOBILE DEVICE ERASER	BLANCCO VIRTUAL MACHINE ERASER, LUN ERASER, FILE ERASER, BLANCCO REMOVABLE MEDIA
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	This method was defined by the US Department of Defense. The 3-pass system writes 0s, 1s and a random character and includes a verification after each pass.	✓	✓	✓
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.	✓	✓	✓
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.	✓	✗	✗
Factory Reset	n/a	A factory reset sets aside previous user data to remove visibility in the user interface; however, the data remains on the device.	✗	**Android, Apple iOS, Blackberry**	✗
Mobile Cryptographic Erasure	n/a	If a device has been previously encrypted, Mobile Cryptographic Erasure will erase the encryption key, rendering the data unrecoverable. While Apple devices and Android devices 7.0 and higher are encrypted by default, most Android devices under 7.0 have not been encrypted and therefore cannot support Mobile Cryptographic Erasure.	✗	**Android 7.0+, Apple iOS**	✗
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.	✓	✗	✗

continued...

			BLANCCO DRIVE ERASER	BLANCCO MOBILE DEVICE ERASER	BLANCCO VIRTUAL MACHINE ERASER, LUN ERASER, FILE ERASER, BLANCCO REMOVABLE MEDIA
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	2	Used by the British Government, this 2-pass overwrite consists of writing a zero and then a random character. This process is completed by verifying the write.	✓	✓	✓
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.	✓	✓	✓
NIST 800-88 Clear	1	The National Institute of Standards and Technology Clear requires the removal of hidden drives (HPA/DCO, if existing). The data is then overwritten and verified.	✓	✗	✗
NIST 800-88 Purge	1	This method requires the removal of hidden drives (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.	✓	✗	✗
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.	✓	✓	✓

continued...

			BLANCCO DRIVE ERASER	BLANCCO MOBILE DEVICE ERASER	BLANCCO VIRTUAL MACHINE ERASER, LUN ERASER, FILE ERASER, BLANCCO REMOVABLE MEDIA
Peter Gutmann's Algorithm	35	Gutmann's Algorithm uses a 35-pass overwrite. The first and last four use random characters, while passes 5-31 use patterns designed with a specific magnetic media encoding scheme in mind. The patterns apply alternating magnetic fields to degauss the drive's material.	✓	✓	✓
U.S. Army AR380-19	3	This method was originally defined by the US Army and uses a 3-pass system uses a random character, a specified character and the complement of the specified character. This process is completed by verifying the write.	✓	✓	✓