

Blank ist konform

**Es gibt Dutzende von Standards für die Datenlöschung,
die auch Ihr Unternehmen betreffen können.**

Unabhängig davon, welche Standards Sie verwenden, können Sie sicher sein,
dass unsere Software damit umgehen kann.



**Moderne Unternehmen verfügen über unterschiedliche Datenspeicherkapazitäten und
ebenso unterschiedliche Compliance-Anforderungen für die Bereinigung dieser Daten.**

Blank ist konform, weil es eine Lösung für Dutzende von Normen bietet.

Die Compliance-Anforderungen für die Datenverwaltung enden nicht, wenn Ihre IT-Anlagen außer Betrieb genommen werden.

Es gibt zahlreiche Standards für die Datenlöschung und das Löschen von Daten von PC-Festplatten, Wechselmedien, LUNs und anderen Speichergeräten. Strenge Standards für diese Datenbereinigungsverfahren werden von Regierungsbehörden und privaten Organisationen auf der ganzen Welt festgelegt.

Diese Standards schreiben vor, wie diese Daten gehandhabt werden, auch wenn die Anlagen nicht mehr im Firmennetz sind und nicht mehr aktiv genutzt werden.

Blank ist konform, weil es Ihnen ermöglicht, Ihre Daten nach dem Standard zu bereinigen, der den Anforderungen Ihres Unternehmens am besten entspricht - - und das Löschzertifikat als Beweis dafür liefert.

Nehmen Sie Ihre IT außer Betrieb? Sie brauchen einen Löschestandard

Um Qualität und Konsistenz zu gewährleisten, werden von Regierungsbehörden und privaten Institutionen **Standards** festgelegt. Was die Datenlöschung betrifft, so unterscheiden sich die Standards normalerweise hinsichtlich der Anzahl der Überschreibungen und des Musters, nach dem ein Datenspeichergerät überschrieben wird.

Die bekanntesten Datenbereinigungsstandards oder -richtlinien sind die 3- und 7-Pass-Methoden des US-Verteidigungsministeriums (DoD 5220.22-M/ECE) und die NIST SP 800-88, Rev. 1 Clear and Purge-Standards, aber in verschiedenen Regionen oder Branchen können auch andere Standards beliebter sein.

Die neueste Version der Datenbereinigung ist IEEE 2883-2022 von der IEEE Standards Association.

Dieser **IEEE-Standard für die Speicherbereinigung** "spezifiziert Methoden zur Bereinigung logischer und physischer Speicher sowie technologiespezifische Anforderungen und Anleitungen für die Beseitigung aufgezeichneter Daten."

Sehen Sie sich die nachstehenden Standards für die Datenlöschung an und entscheiden Sie dann, welche(r) für Ihr Unternehmen am besten geeignet ist/sind.

Standard Name	# Anzahl der Durchgänge	Beschreibung
Sicherheitsanweisung für das Truppsystem 5020	2	Ursprünglich von der United States Air Force definiert, wird dieses 2-Pass-Überschreiben durch die Verifizierung des Schreibvorgangs abgeschlossen.
Aperiodisches zufälliges Überschreiben/Zufall	1	Bei diesem Vorgang werden die Daten mit einem zufälligen statt mit einem statischen Muster überschrieben. Jeder Sektor des Laufwerks enthält andere Daten. Dieser Vorgang wird durch die Verifizierung des Schreibvorgangs abgeschlossen.
Blancco SSD-Löschung	Proprietär	Der mehrstufige, proprietäre SSD-Löschansatz von Blancco nutzt alle unterstützten SSD-Sicherheitsprotokolle. Diese innovative Methode umfasst mehrere zufällige Überschreibungen, Löschung auf Firmware-Ebene, Aufhebung der Einfriersperre und vollständige Überprüfung.
Der Algorithmus von Bruce Schneier	7	Bei diesem vom Sicherheitsexperten Bruce Schneier vorgestellten 7-stufigen Verfahren werden 1en, 0en und ein Strom zufälliger Zeichen überschrieben.

Standard Name	# Anzahl der Durchgänge	Beschreibung
BSI-2011-VS	4	Dieses 4-Pass-System ist der ursprüngliche BSI-Standard, der vom deutschen Bundesamt für Sicherheit in der Informationstechnik definiert wurde.
BSI-GS	1	Dieser vom deutschen Bundesamt für Sicherheit in der Informationstechnik definierte Prozess beginnt mit dem Entfernen versteckter Laufwerke (HPA/DCO, falls vorhanden) und dem Überschreiben mit aperiodischen Zufallsdaten. Im nächsten Schritt wird je nach Laufwerkstyp ein Firmware-basierter Befehl ausgelöst. Der letzte Schritt ist die Verifizierung des Schreibvorgangs.
BSI-GSE	2	Der BSI-GSE fügt dem BSI-GS einen zusätzlichen Schritt hinzu: Nach dem ersten Überschreiben wird ein weiteres Überschreiben mit aperiodischen Zufallsdaten hinzugefügt, bevor die letzten beiden Schritte folgen.
CESG CPA - Höhere Stufe	3	Der Standard der National Technical Authority for Information Assurance der britischen Regierung ist ein dreistufiger Prozess mit einer Überprüfung nach jedem Schritt.
Kryptografische Löschung (Crypto Erase)	K/A	Bei dieser Methode wird der systemeigene Befehl zum Aufrufen einer kryptografischen Löschung verwendet, die den Verschlüsselungsschlüssel löscht. Die verschlüsselten Daten verbleiben zwar auf dem Speichergerät selbst, können aber nicht entschlüsselt werden, so dass die Daten nicht wiederherstellbar sind. Da diese Methode die vom Hersteller definierten nativen Befehle verwendet, ist sie nur verfügbar, wenn sie von dem zu löschenden Laufwerk unterstützt wird.

Standard Name	# Anzahl der Durchgänge	Beschreibung
DoD 5220.22-M	3	Das vom US-Verteidigungsministerium (DoD) im National Industrial Security Program Operating Manual (auch bekannt als DoD-Dokument Nr. 5220.22-M) veröffentlichte Verfahren zum Überschreiben von Festplattenlaufwerken (HDD) mit Mustern aus Einsen und Nullen. Der Prozess erforderte drei sichere Überschreibungsdurchgänge und eine Überprüfung am Ende des letzten Durchgangs. Weitere Informationen zu diesem Standard finden Sie in unserem Blog, "Everything You Need to Know About the DoD 5220.22-M Disk Wiping Standard & Its Applications Today."
DoD 5220.22-M ECE	7	Bei dieser Methode handelt es sich um eine erweiterte (7-Durchgänge) Version der DoD 5220.22-M. Sie führt die DoD 5220.22-M zweimal durch, wobei ein zusätzlicher Durchgang (DoD 5220.22-M (C) Standard) dazwischen geschoben wird.
Erweiterte Firmware-basierte Löschung	3	Dieser von Blanco definierte Standard fügt ein Überschreiben als ersten Schritt hinzu und folgt dann dem Standard Firmware Based Erasure, so dass es sich um einen 3-Schritt-Prozess handelt.
Firmware-basierte Löschung	2	Dieser Blanco-definierte Standard ist ein zweistufiger Prozess, der einen Firmware-Befehl auslöst, der vom Laufwerkstyp abhängig ist. Der letzte Schritt des Prozesses ist die Verifizierung des Schreibvorgangs.
HMG Infosec Standard 5, Höherer Standard	3	Dieser von der britischen Regierung verwendete 3-Pass-Überschreibvorgang fügt einen zusätzlichen Schreibvorgang hinzu. Wie bei der Basisnorm wird dieser Vorgang durch die Überprüfung des Schreibvorgangs abgeschlossen.
HMG Infosec Standard 5, Unterer Standard	1	Dieses von der britischen Regierung verwendete Verfahren zum Überschreiben in einem Durchgang besteht aus dem Schreiben eines Nullmusters. Dieser Vorgang wird durch die Verifizierung des Schreibvorgangs abgeschlossen.

Standard Name	# Anzahl der Durchgänge	Beschreibung
IEEE 2883-2022 Klar	0-2	Das von der IEEE Standards Association entwickelte Verfahren IEEE Clear erfordert die Entfernung/ Löschung bestimmter Bereiche (z. B. versteckte Bereiche, entvölkerte Speicherelemente oder Cache-Zonen, sofern vorhanden). Die Daten werden dann bereinigt (über einen Firmware-basierten Befehl oder durch Überschreiben) und verifiziert. Weitere Informationen finden Sie in unserem Artikel " New IEEE Data Erasure Standard Fills Technology Gap "
IEEE 2883-2022 Säubern	0-2	IEEE Purge wurde von der IEEE Standards Association , entwickelt und erfordert die Entfernung/Löschung bestimmter Bereiche (z. B. versteckte Bereiche, entvölkerte Speicherelemente oder Cache-Zonen, falls vorhanden). Die Daten werden dann (über einen firmwarebasierten Befehl) bereinigt und überprüft. Weitere Informationen finden Sie in unserem Artikel " New IEEE Data Erasure Standard Fills Technology Gap "
Nationales Zentrum für Computersicherheit (NCSC-TG-025)	3	Dieses von der Nationalen Sicherheitsbehörde der USA definierte 3-Pass-System umfasst nach jedem Durchgang eine Überprüfung von 0en, 1en und einem Zufallszeichen.
Veröffentlichung des Marine-Stabsbüros (NAVSOP-5239-26)	3	Dieses von der US Navy veröffentlichte 3-Pass-System verwendet ein bestimmtes Zeichen (und sein Komplement) sowie ein Zufallszeichen. Der Prozess wird durch die Verifizierung des Schreibens abgeschlossen.
NIST 800-88 Klar	0-2	Das National Institute of Standards and Technology Clear verlangt die Entfernung von versteckten Bereichen (HPA/DCO, falls vorhanden). Die Daten werden dann überschrieben und verifiziert.
NIST 800-88 Bereinigung	0-2	Diese Methode erfordert die Entfernung von versteckten Bereichen (HPA/DCO, falls vorhanden). Je nach Laufwerkstyp wird ein Firmware-basierter Befehl ausgelöst, und der letzte Schritt ist die Verifizierung des Schreibvorgangs. Unser NIST-Leitfaden enthält weitere Einzelheiten.

Standard Name	# Anzahl der Durchgänge	Beschreibung
NSA 130-1	3	Diese von der National Security Agency definierte Methode verwendet ein 3-Pass-Überschreibeverfahren: Schreiben eines zufälligen Zeichens, Schreiben eines weiteren zufälligen Zeichens und Schreiben eines bekannten Wertes. Dieser Prozess wird durch die Verifizierung des Schreibvorgangs abgeschlossen.
OPNAVINST 5239.1A	3	Dieser von der US Navy definierte Prozess wird durch die Überprüfung des Schreibvorgangs nach einem 3-fachen Überschreiben abgeschlossen - das erste Byte wird zufällig und die letzten beiden statisch überschrieben.

Benötigen Sie einen speziellen Standard für die Datenlöschung und -vernichtung? Wir haben das Richtige für Sie.

Als weltweiter Marktführer im Bereich der zertifizierten Datenlöschung unterstützt Blanco mehr als 24 internationale Standards für die Datenlöschung, die von Regierungsbehörden, Justizbehörden und unabhängigen Testlabors festgelegt wurden, darunter alle oben genannten.

Unabhängig von dem/den internen Standard(s), der/die von Ihrer Regierung oder Organisation gefordert wird/werden, können Sie mit den Lösungen von Blanco die Einhaltung der Vorschriften nachweisen und Ihre Daten schützen.

Die Blanco-Perspektive

Während sich die Standards und Anforderungen mit der Technologie weiterentwickeln, ist Blanko konform, weil es konsistent ist.

Die neuesten IEEE 2883-2022 Standards werden nicht die letzten sein, aber sie sind die besten für den nachhaltigen Schutz von Daten auf neueren, stillgelegten Anlagen.

Mit der Weiterentwicklung neuer Technologien werden wir auch weiterhin neue Möglichkeiten entwickeln, um die Sanierungsanforderungen zu erfüllen, denen Unternehmen zum Schutz ihrer Daten folgen.

Bleiben Sie auf dem Laufenden über Compliance

Bleiben Sie auf dem Laufenden über die neuesten Datenschutzanforderungen und gesetzlichen Änderungen, die Ihr Unternehmen betreffen könnten.

Besuchen Sie unseren Content Hub