blancco

Data Erasure FAQs for the U.S. Public Sector

Blancco has been helping government organizations across the globe reduce risk for over twenty years. As the leader in data erasure software, our solutions are proven to be the most secure and effective on the market. Read on for a list of some of the common questions we receive from U.S. public sector, then reach out to us for additional information on how we can help you improve data security across your organization.

Which is more secure – physical destruction or data erasure?

While physical destruction is required for many government organizations, newer drive technology presents additional variables that need to be considered to mitigate risk. While degaussing is the cheapest and easiest form of physical destruction for HDDs, it is incapable of removing data on SSDs or NVMes. Degaussing destroys data by reducing or eliminating the unwanted magnetic fields and rendering the drive unusable. Flash-based storage such as SSDs or NVMes are incapable of being degaussed because their data is not stored magnetically.

As NIST explains, "Destructive techniques for some media types may become more difficult or impossible to apply in the future. Traditional techniques such as degaussing (for magnetic media) become more complicated as magnetic media evolves, because some emerging variations of magnetic recording technologies incorporate media with higher coercivity (magnetic force). As a result, existing degaussers may not have sufficient force to effectively degauss such media."

Physically shredding flash storage presents security challenges, as the density of data per drive is progressively increasing while the drive size is decreasing. Typically, a shred width of 1/2" or smaller is needed to break through the small memory chips and securely remove the data. Most standard industrial shredders will only shred to 1" particle size—leaving data behind and available for hackers to restore with the right means.

Again, as NIST explains, "Applying destructive techniques to electronic storage media (e.g., flash memory) is also becoming more challenging, as the necessary particle size for commonly applied grinding techniques goes down proportionally to any increases in flash memory storage density. Flash memory chips already present challenges with occasional damage to grinders due to the hardness of the component materials, and this problem will get worse as grinders attempt to grind the chips into even smaller pieces."

Security throughout the full chain of custody can also be an issue. Tracking an asset at every step of its end-of-life journey (including during transportation to an off-site facility), is of the utmost importance. Sanitizing data on-site mitigates this risk, while also providing a full audit trail prior to destruction.

During the lifecycle of data, there are numerous levels of security to protect the integrity of that data (firewalls, encryption, etc). We take the same approach at the end-of-life or end-of-lifecycle by adding an additional layer of security by combining secure erasure and physical destruction in tandem, if physical destruction is required by regulation. That way, you're adding an extra layer of secure protection to assets before they meet their demise.

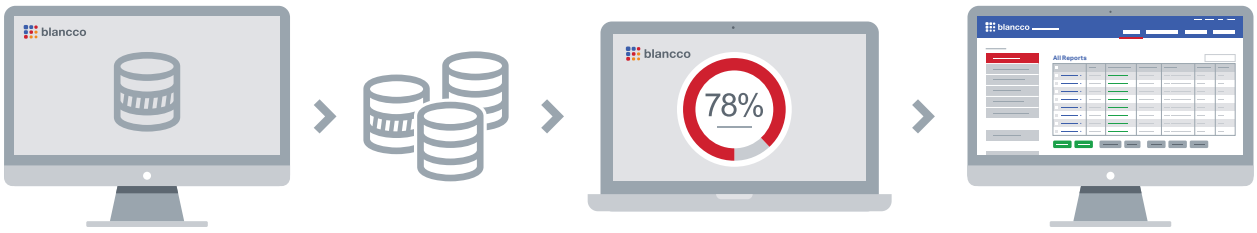
How does secure data erasure result in monetary savings?

The average lifespan of a laptop is around four years, meaning 25 percent+ of an organization's laptops are reaching end-of-life every year. Physically destroying valuable laptops, PCs, mobile phones and other IT assets not only comes with security risk (and a cost)—but also doesn't give local public sector organizations the opportunity to erase and reuse those assets internally (saving money) or donate them to local schools in need. Simply storing assets with private data isn't a great idea, either, as it can lead to sensitive data leaks. Data erasure is the only way to guarantee data sanitization across your IT assets with the confidence to reuse, resell or recycle them. And with Blancco's scalable, plug-and-play solution, you won't need to spend a lot of time or money on training employees.

How many overwrites are required for secure erasure?

Multiple overwrites are not necessary today, thanks to advances in technology. The common DoD standard does not account for newer technologies (such as SSDs) and recommends a three-pass method. However, the more recent NIST standard is now the go-to standard for the industry, as it takes newer technologies into account and has essentially replaced DoD requirements. This standard recommends a single, secure overwrite. Blancco offers both of these standards, along with 20+ others, allowing organizations the ability to choose the most effective, efficient method for their specific needs.

Which Blancco solutions are a fit for service providers serving public sector organizations?



Deploy
via Local Area Network or On-Site

Perform
using Blancco Drive Eraser, File Eraser, LUN Eraser or Virtual Machine Eraser

Track
using Blancco Management Console

1. **Erasure-as-a-Service Solutions – Easy, worry-free deployment of Blancco data erasure solutions.**

   Erase sensitive data on SSDs and HDDs in laptops, PCs and servers with Blancco Drive Eraser. Or, erase data in live environments with Blancco LUN Eraser and VM Eraser Solutions. With Blancco's Erasure-as-a-Service Offering through Blancco's Service Provider partner program, you can:

   Deploy:

   - Deploy software via Windows PE, WIN installment, MSI, PXE boot, CD or USB.
   - Employ organization-specific erasure policies via our configurable software.
   - Take advantage of integration with Active Directory and existing ticketing systems via Blancco's patent-pending two-way communication. There's no need to add or train on additional software

   Perform:

   - Customize workflows for different types of technologies.
   - Streamline data erasure regardless of operating system or manufacturer.
   - Choose from 22 erasure standards to meet internal and external data sanitization requirements Including DOD + NIST.
   - Erase a wide range of data storage devices, from HDDs and standard SSDs to NVMe to PCIe-based SSDs, to removable media (USBs, SDs), VMs and files.

   Track:

   - Store a tamper-proof Certificate of Erasure for every IT asset erased.
   - Automatically send erasure reports to the Blancco Management Console or your asset management system.
   - Choose from a variety of report types including CSV, XML or PDF; send these to clients, or track internally.
   - Achieve compliance with local, national and global data security and privacy regulations and guidelines.

All Blancco Erasure-as-a-Service Solutions come with data erasure management and support.

2. **Blancco File Eraser**

   Erase sensitive data (including files and folders) in active environments on assets such as LUNs, servers and VMs, as well as laptops and desktops. Several law enforcement organizations across the globe are using these active erasure services in a unique way—by erasing the sensitive data on cameras when it reaches its retention date or is no longer necessary. Blancco File Eraser can also be used to clear temporary files on laptops daily, or as retention policies require. Erasures can be automatically scheduled to occur per your internal policies.

3. **Blancco Hardware Solutions (through Erasure-as-a-Service)**

   Securely erase data on loose drives and drive enclosures on-premise at data centers or in large IT facilities. Our data erasure appliances provide the most trusted solution for on-site data sanitization requirements using a quick and effective process. When your organization invests in Blancco Hardware solutions via our Erasure-as-a-Service offering, you'll have access to secure on-site data erasure services, including deployment, performance, tracking and support.

Why Blancco?

Blancco is the industry standard in data erasure and mobile device diagnostics. Blancco data erasure solutions provide thousands of organizations with the tools they need to add an additional layer of security to their endpoint security policies through secure erasure of IT assets. All erasures are verified and certified through a tamper-proof audit trail.

Blancco data erasure solutions have been tested, certified, approved and recommended by 18 governing bodies and leading organizations around the world. No other data erasure software can boast this level of compliance with the rigorous requirements set by government agencies, legal authorities and independent testing laboratories.

Contact us today to learn more about our solutions for U.S. public sector organizations.