Top 10 Public Sector Questions

The public sector has particular requirements for data eradication. WipeDrive has been helping government agencies reach these conditions for over ten years. As the proven wipe tool of choice for US and Canadian governments, the solution will fit perfectly in your environment and be easy to implement. This is a list of the top 10 questions the public sector faces when choosing a data wipe solution.

1: Why does WipeDrive Enterprise offer government agencies the freedom to save audit reports to any location they prefer?

A: WipeDrive Enterprise focuses on client access to all their data. The software does not store log files in a proprietary system but allows users to setup the type of audit trail (PDF, XML, TXT, CSV, HTML or DB) and save it to any location they prefer. Clients can then provide these reports to internal resources for audits or to clients for proof of erasure.

The implementation of Consoles and Management Systems can be cumbersome. WipeDrive Enterprise has followed the client's recommendations and provides the freedom to save log files to any destination they prefer, without a license tracking mechanism.

2: Why are low cost erasure solutions inferior to WipeDrive's?

A: The cost of a license should be directly tied to the benefit and value of that software tool. These low cost erasure solutions are mostly meant for home use and lack the certifications needed for proper data destruction. Also, they have errors processing large quantities of systems and new drive technology.

All our clients that have migrated from a low-cost/free tool have seen substantial gains from a less expensive processing system and increasing the throughput by higher compatibility matrix. We strongly caution against these low-cost tools – a mistake here can lead to data breaches and other major issues.

globallifecycle SOLUTIONS-EMEA

3: Why should an agency choose data erasure over physical destruction?

A: Physical destruction is the primary choice of most government agencies, but it has many negatives.

- The largest downside is destroyed drive have no resale/donation value left.
- Degaussing is a very cheap and affordable method of destruction, but it is not effective on SSD or NVMe (any flash-based storage) drives.
- The flash chips on SSD & NVMe drives are so small that if a shredder does not grind to a specific particulate size, it is possible for the chip to make it through the shredding process.

The major issue with physical destruction is the chain of custody. All data-bearing devices must be properly managed until they are destroyed. Typically, this means a locked basement storage locker contains very sensitive data. If a malicious actor was able to gain access to these devices or the devices were lost by accident, it could carry serious consequences.

We recommend first wiping the data-bearing device onsite (at the time of decommission) and then process the drive through physical destruction or your resale process. This lessens the chance of a data breach and provides a wipe report for administrator reference.

With secure erasure, the end-of-life process can provide a reliable method to ensure data security prior to physical destruction or as an alternative.

4: How can a government agency save monetarily by implementing secure data sanitization?

A: Government agencies follow approved lifecycle plans for all their IT assets. By moving from physical destruction to data wiping (using the SP 880-88 R1 as a guide) the public sector can resell or donate IT assets that would otherwise be destroyed. This provides a monetary increase for the budget or allows the public sector organization to donate IT assets to a local school or charity.

The WipeDrive solution provides a certified, proven solution that is easy to implement at all agency locations and provides a tamper-proof audit report to the administrators.

globallifecycle SOLUTIONS·EMEA

5: How quickly should a wipe complete?

A: Storage media has a variety of sizes from 250GB to 16TB. A full-featured erasure tool should be able securely overwrite any device at 30-40GB per minute. New flash media and encryption removal technology can make this process even faster. Be wary of low-cost tools, they typically lack the drivers and ATA commands to quickly and efficiently erase any storage device.

6: How many times should a government agency wipe a computer?

A: According to NIST SP 880-88 R1, a single overwrite with ATA commands and a 10% verify will satisfy their requirements for a secure overwrite pattern.

7: How long should audit reports be stored?

A: Audit reports should be stored a minimum of seven (7) years or as otherwise stipulated by government regulations.

8: Does the public sector need to verify erasures?

A: Government agencies should consistently be checking drive wipe results to ensure that data erasure tools are functioning correctly on new hardware. There are no regulations that require 3rd party verification of erased drives but it is always a good policy.

9: How does a US-based and UK-based Support Team help WipeDrive assist Government Agencies?

A: The Support Teams for WipeDrive cover most business hours around the globe and this means government agencies will receive direct phone access for their issues. WipeDrive also provides Support in Chat and Email.

globallifecycle SOLUTIONS-EMEA

10: How easy is it to get WipeDrive setup?

A: WipeDrive is a boot and run program that could be implemented in minutes. Government employees have found it extremely easy to become familiar with WipeDrive. We also offer User Training Classes and Admin I and Admin II Certification for those that need additional training and certification.

BONUS: How quickly can Public Sector Clients receive new custom builds and deployments from WipeDrive?

A: The WipeDrive Support Team is trained on providing custom builds and PXE/CD/USB/Remote deployments immediately. Receiving a new build is a simple as an email/chat/call and the build can be delivered in minutes. If there are major customizations, the WipeDrive Support Team will work with the agency on a delivery date.