ENCRYPTED USB STORAGE SOLUTIONS FOR
FEDERAL GOVERNMENT AGENCIES AND CONTRACTORS

IRONKEY™

KINGSTON'S SECURE STORAGE

IS YOUR MOBILE WORKFORCE PUTTING YOU AT RISK?

Workforce mobility equates to productivity, efficiency and flexibility. But it also brings risk: You can't afford to let mobile workers compromise the security of the sensitive data they carry.

No wonder Federal government, military and intelligence agencies are required to meet stringent requirements that cover data confidentiality, integrity, and availability. U.S. legislative mandates, international data security requirements, the Federal Information Processing Standard (FIPS), and various state data security directives have all combined to make protecting sensitive information your responsibility.

AVOID THE HIGH COST OF NON-COMPLIANCE

Failing to comply with data security mandates can trigger serious problems for agencies, including a loss of public trust, more intense oversight by regulators, and costly class-action lawsuits. And for civilian companies that work with Federal agencies, non-compliance could result in lost contracts, lay-offs and worse.

GET TRUE MOBILE PROTECTION WITH KINGSTON

With Kingston's encrypted USB drives which include industry favorites from Ironkey, you can simplify compliance by relying on a full range of products that include the right solution to meet every need. Kingston's encrypted line of drives feature products that range from Entry level Alphanumeric keypad PIN protection all the way through FIPS 140-2 Level 3* validated, military-grade encrypted USB storage devices. Kingston lets you put a wall between unauthorized users and the data you need to protect.

Choose from an array of Kingston IronKey and DataTraveler solutions:

- Hardware based encrypted USB flash drives
- FIPS Certification 197 through 140-2 Level 3 (Drive specific)
- Device Management integration seamlessly through DataLocker EMS and SafeConsole products.

To find out more about the entire line of Kingston Ironkey and Kingston DataTraveler Encrypted USB drives, please visit www.Kingston.com/encrypted

GET THE KINGSTON ADVANTAGE

Mobilize employees and contractors by enabling them to safely access agency data from virtually any PC and tablet.

Shield government data with a virtually indestructible drive that exceeded military waterproof testing requirements.

Lock down sensitive data by putting military-grade encryption and a ruggedized enclosure between unauthorized users and your Kingston IronKey drive's contents.

Meet security mandates by relying on FIPS 140-2 Level 3* validated devices and advanced auditing and reporting.

Centrally manage data access and use, no matter where employees go.

Maintain critical operations during severe weather or other disasters.

WITH KINGSTON SECURE STORAGE DRIVES...

- Employees can access data from home using virtually any PC.
- Federal law enforcement personnel can review and update case files in the office or in the field.
- Scientists, analysts and forecasters can access data sets from any location with a PC or tablet.
- Contractors can work at agency offices while still having trusted access to data.
- Agencies can maintain operations during disasters by putting critical data in the hands of key personnel.
- IT can enforce access and use policies from a central console.
- IT can demonstrate best effort to comply with new and unsettled regulations, including the GDPR.

Kingston TECHNOLOGY