ENCRYPTED USB STORAGE SOLUTIONS FOR
FEDERAL GOVERNMENT AGENCIES AND CONTRACTORS

IRONKEY™

IRONKEY™ 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 IRONKEY

With IronKey, you can simplify compliance by relying on FIPS 140-2 Level 3* validated, military-grade encrypted USB storage devices that put a wall between unauthorized users and the data you need to protect. Choose from an array of IronKey solutions:

- encrypted USB flash drives
- encrypted USB external hard drives
- USB drive management solutions

IronKey devices offer multiple layers of protection, including: strong, multifactor authentication (password and biometric); XTS-AES and AES 256-bit hardware encryption; and tamper- and waterproof** enclosures.

GET THE IRONKEY 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 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 IRONKEY 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.

BUILD YOUR SECURITY MOBILE STORAGE STRATEGY WITH IRONKEY

ENCRYPTED USB FLASH DRIVES 2GB-128GB

HIGHEST SECURITY (FIPS 140-2 LEVEL 3)* + CENTRALIZED MANAGEMENT	*The right choice for . . .*
IRONKEY ENTERPRISE S1000 USB 3.0 performance with cloud or on-premises centralized management, enhanced XTS-AES 256-bit encryption, optional antivirus and lifetime warranty	• Auditing and reporting for compliance with widest range of data security mandates • Broad deployments • High-risk, high-traffic environments
IRONKEY ENTERPRISE S250 + D250 Cloud or on-premises centralized management, optional antivirus, ID management and VeriSign® Identity Protection (VIP)	
IRONKEY F150 Rugged metal enclosure, optional centralized management and antivirus	
IRONKEY F100 Durable polymer housing, optional centralized management and antivirus	• Affordable deployment • Compliance with strict data security mandates

HIGHEST SECURITY (FIPS 140-2 LEVEL 3)*	*The right choice for . . .*
IRONKEY BASIC S1000 USB 3.0 performance, enhanced XTS-AES 256-bit encryption, lifetime warranty	• Deployments without the need for centralized management, reporting or auditing • High-risk, high-traffic environments • Compliance with most data security mandates
IRONKEYBASIC S250 + D250 Self-service password reset	

***What is FIPS 140-2 Level 3?** A U.S. government computer standard that defines a high level of cryptographic and physical protection designed to keep sensitive data safe from theft or hacking. For a listing of IronKey certificate numbers, please visit http://www.ironkey.com/en-US/website/certification-and-compliance.html.

****What is the waterproof standard?** MIL-STD-810G/MIL-STD-810F, also referred to as US Department of Defense Test Method Standard for Environmental Engineering Considerations and Laboratory Tests, establishes testing standards to evaluate the durability of products, especially in extreme circumstances. IronKey devices are waterproof and dustproof according to MIL-STD-810G/MIL-STD-810F standards.

STAY IN CONTROL OF DEVICES AND DATA

With the optional cloud-based or on-premise IronKey Enterprise Management Service or Server, you can centrally administer access and usage policies across thousands of IronKey USB drives. Force password changes, re-commission drives no longer in use, even remotely disable or terminate rogue drives. Simplify compliance with advanced reporting and auditing that lets you document how, where and when users have accessed, saved or modified confidential data.

DEPLOY TOUGH, PROVEN IRONKEY DRIVES

IronKey USB flash drives undergo thousands of hours of rigorous read/write tests, and we encase each one in a sturdy, tamper-proof chassis that's water, dust and shock-proof.

RELY ON AN END-TO-END IRONKEY SOLUTION

IronKey solutions are designed to work seamlessly together and create a cost-effective, end-to-end solution that you can use to reduce your potential exposure to non-compliance, drive down operating costs, improve productivity, and maintain operations no matter what happens. Deploy our encrypted USB storage devices in conjunction with secure portable workspace products to fully and confidently mobilize any workforce.

THIS DOCUMENT SUBJECT TO CHANGE WITHOUT NOTICE
©2016 Kingston Technology Corporation, 17600 Newhope Street, Fountain Valley, CA 92708 USA, All rights reserved.
All trademarks and registered trademarks are the property of their respective owners.