

IRONKEY™ SECURE STORAGE



MINIMIZE THE RISK OF MOBILITY

Financial services firms are rapidly transitioning from stationary workplaces to environments that empower employees and contractors to work from anywhere – at the office, at home or on the road. But without taking measures to secure sensitive financial data, customer records or intellectual property, banks, brokerages, payment card companies, insurers and credit clearinghouses may find mobility brings more risk than they anticipated.

CAN YOU AFFORD THE COST OF NON-COMPLIANCE?

Financial services companies face a growing number of regulatory mandates for ensuring customer data and other information doesn't fall into the wrong hands. From the Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley Act (SOX) to the Payment Card Industry Data Security Standard (PCI DSS) and multiple state laws, banks, insurers and other institutions face considerable penalties for non-compliance.

In fact, failing to comply with these regulations costs over 2.5 times more than the cost of compliance (2011 Ponemon Study). And while fines and penalties can hurt, they pale when compared to the cost to your brand and your business when customers fear they trust you with their personal information.

PRESERVE DATA, AND YOUR REPUTATION

IronKey helps you preserve what's important. Our military-grade encrypted USB storage devices 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, XTS-AES and AES 256-bit. hardware encryption, and tamper- and waterproof** enclosures.

EASE THE BURDENS OF COMPLIANCE

Complying with data security regulations needn't be a burden. Use IronKey's advanced reporting and auditing capabilities to document how, where and when users have accessed, saved or modified confidential data. And for maximum flexibility, we offer both premise-based management solutions (when device management must reside behind your firewall) and cloud-based management solutions (which eliminate the need for capital investments in servers and other hardware).

GET THE IRONKEY ADVANTAGE

Mobilize executives, loan officers, adjusters and others by enabling them to safely access data and applications from virtually any PC or tablet.

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

Lock down sensitive financial 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.

Simplify compliance with advanced auditing and reporting capabilities.

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

WITH IRONKEY SECURE STORAGE DRIVES...

- Teleworkers can safely access data and applications from home.
- Banks, insurers and others can equip contractors to work in the field without investing in laptops or tablets.
- Auditors can gain trusted access to sensitive data when on assignment or when working from home.
- Claims adjusters, examiners and investigators can have access to data and applications from the field.
- Organizations can provide key personnel with access to critical data to maintain operations if severe weather or other disasters strike.
- 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

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

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

HIGHEST SECURITY (FIPS 140-2 LEVEL 3)*

IRONKEY BASIC S1000

USB 3.0 performance, enhanced XTS-AES 256-bit encryption, lifetime warranty

IRONKEYBASIC S250 + D250

Self-service password reset

The right choice for . . .

- Auditing and reporting for compliance with widest range of data security mandates
- Broad deployments
- High-risk, high-traffic environments

- Affordable deployment
- Compliance with strict data security mandates

The right choice for . . .

- Deployments without the need for centralized management, reporting or auditing
- High-risk, high-traffic environments
- Compliance with most data security mandates

***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.

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.