ENCRYPTED USB STORAGE SOLUTIONS FOR EDUCATION

IRONKEY™ SECURE STORAGE

KNOW THE HIGH PRICE OF DATA BREACHES

From K-12 districts to four-year universities, educational institutions house volumes of personal information about students, faculty and staff. Credit card details, Social Security Numbers, grades and employment records — all can too easily fall into the wrong hands.

No wonder schools and other institutions must comply with regulations such as the Family Educational Rights and Privacy Act (FERPA) and the Payment Card Industry Data Security Standard (PCI DSS).

But when breaches do happen, the price can be high. Data breaches can trigger losses in research funding, threaten public-private partnerships, expose students and employees to identity theft, and deal serious blows to your reputation.

HOW DO YOU REIN IN A WIDE-OPEN ENVIRONMENT?

But education presents unique security challenges. Many institutions decentralize their IT operations across campuses or departments, and school-owned computers are physically available to dozens of people every day. Add mobility to the mix – with employees teleworking from home or other campuses, researchers moving from the lab to the field, and students bringing school computing home – and threats to your data, applications or networks multiply quickly.

COUNT ON IRONKEY TO KEEP DATA SAFE

With IronKey, you'll keep data where it belongs. 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 FERPA or PCI DSS requirements 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 faculty, staff, researchers and others by enabling them to safely access data and applications from virtually any PC.

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

Protect personal student and research data by putting military-grade encryption and a ruggedized enclosure between unauthorized users and your IronKey drive's contents.

Safeguard digital identities to prevent costly fraud or IP theft.

Comply with privacy regulations by relying on FIPS 140-2 Level 3* with advanced auditing and reporting.

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

WITH IRONKEY SECURE STORAGE DRIVES...

- Faculty, staff and students can safely access data from home using virtually any PC or tablet.
- Researchers can update results at the lab, in the field, in an office, in the classroom or at home.
- Faculty can access institutional applications, data and more while attending conferences or symposiums.
- Administrators always have trusted access to data and applications.
- Adjunct faculty can securely work with institutional records and applications anywhere they have access to a any PC or tablet.
- Institutions can provide key personnel with 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	*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.

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.