A CERTIFIED WINDOWS PORTABLE DESKTOP
FOR FEDERAL AGENCIES AND CONTRACTORS

IRONKEY™ by imation

IRONKEY™ WORKSPACE

SUPPORT COMPLIANCE & KEEP MOBILE WORKERS PRODUCTIVE

HARNESS THE POWER OF MOBILITY, BUT REIN IN THE RISKS.

Federal agencies and contractors with mobile employees are responsible for securing the data and applications those users carry and use. To operate efficiently in an increasingly mobile world, they must give authorized users anytime-access to sensitive data without compromising vital information, core applications or protected networks.

DON'T COMPROMISE COMPLIANCE.

Increasingly, government, defense and intelligence agencies – and the civilian companies that contract with them – are on the hook to:

- Meet U.S. legislative requirements, including the Federal Information Security Management Act (FISMA), FIPS 140-2 Level 3 encryption requirements, OMB M-06-16 Mandate, Federal Desktop Core Configuration (FDCC) mandates, and the Director of Central Intelligence Directive (DCID) 6/3.
- Comply with the Telework Enhancement Act of 2010 requiring that every U.S. government employee work from home to the maximum extent possible.
- Meet HSPD-12 requirements to use your government issued smart card identity credentials to access federal information systems.
- Show compliance with an array of international data security requirements. Agencies can't afford the price of non-compliance: loss of public trust, more intense oversight and costly class-action lawsuits. And contractors who fail to outfit mobile workers with a secure portable workspace risk disqualification from bidding on future government business.

EQUIP EMPLOYEES TO WORK FROM ANYWHERE.

Now there's a solution that equips Federal employees and contractors with a fully functioning version of Windows 10 or Windows 8.1/8 Enterprise—one that delivers a fast, full Windows desktop and can be booted directly from a trusted IronKey USB flash drive. With IronKey Workspace W700, W700SC and W500, you can transform virtually any computer into your employees' own personal workspace capable of using all host system resources—and certified by Microsoft for Windows To Go[1].

- Use a centralized IT Windows image, complete with all your agency's applications, from virtually any computer.
- Enable key personnel to maintain operations during power outages, severe storms, earthquakes, fires, terrorist attacks or other disasters.

PROTECT YOUR DATA, APPLICATIONS, RESEARCH DATABASES AND MORE.

IronKey Workspace W700, W700SC and W500 drives let you control access to your agency's mobile Windows To Go desktops with built-in password protection capabilities and 256-bit XTS-AES Cipher-Block Chained mode hardware encryption. And agencies deploying IronKey Workspace drives can take further control of their portable workspace devices with IronKey's optional centralized management and provisioning platforms[3]

- For agencies with less demanding security requirements, IronKey Workspace W300 and W200 drives feature full-disk encryption and password protection.

WITH IRONKEY WORKSPACE USB FLASH DRIVES...

- Personnel can safely and efficiently work from home using any compatible PC, tablet or Mac.[1]
- Agencies can mobilize employees without having to procure and issue laptops or tablets.
- Federal law enforcement personnel, whether in the office or in the field, can update case files and search databases using a trusted Windows environment.
- Scientists, analysts and forecasters can refresh models and update data sets from work, home or the field.
- Contractors can work at agency offices while still having trusted access to their desktops.
- Managers and directors can securely work with agency applications at any time and from any location with a compatible computer.
- Agencies can distribute full Windows work environments to key personnel to maintain crucial operations if severe weather, terrorist attacks or other disasters strike.
- IT administrators can enforce access and use policies from a central console.

QUICK REFERENCE

IRONKEY WORKSPACE W700, W700SC & W500

PROTECTION OF SENSITIVE DATA

Problem: Breaches of sensitive data are costly. They can expose citizens to identity theft, erode public confidence, and even threaten public safety or national security.

Solution: IronKey Workspace drives help protect your data and your agency by safeguarding portable desktops and data with password protection and and 256-bit XTS-AES hardware encryption. In addition, IronKey Workspace W700 and W700SC drives are FIPS 140-2 Level 3 validated[2]; providing an "above Federal Encryption Standards" level of protection with full device certification. The W700SC drives also feature support for CAC/PIV smart cards so that agencies are in full compliance with HSPD-12.[3]

IT-MANAGED DESKTOPS AND DEVICES

Problem: When mobile workers use home computers or systems in uncontrolled environments, they risk exposing files, networks and applications to unauthorized software and malware.

Solution: IronKey Workspace flash drives let you equip users to work anywhere using environments that are provisioned and managed by IT and that mirror your institution's desktop. Optional enterprise-class administration and mass provisioning platforms give IT management the ability to control drive access and usage, set password policies and deploy large numbers of mobile workspaces.

DEVICE QUALITY

Problem: Too many portable workspace solutions are made with inexpensive, unreliable commodity parts.

Solution: Rugged IronKey Workspace drives undergo thousands of hours of rigorous read/write tests to help ensure users are getting a USB flash drive they can count on. Every drive is assembled in America from quality components, and is encased in a sturdy chassis that's resistant to water, dust and shocks to help protect the drive and its contents from the elements.

MICROSOFT CERTIFICATION

Problem: Solutions that haven't been certified by Microsoft can expose you to conflicts, crashes or worse, and are explicitly not supported by Microsoft.

Solution: IronKey Workspace drives are Microsoft-certified Windows To Go solutions that deliver a true Windows 10 or Windows 8.1/8 desktop protected by a hardware encrypted IronKey USB flash drive. And they're the only solutions built around Imation's portable desktop expertise and the proven dependability of IronKey drives.[4]

HIGH PERFORMANCE

Problem: Many mobile desktops are slow and hard to use.

Solution: IronKey Workspace drives are built for speed, delivering read/write performance exceeding the minimum requirements for Windows To Go devices. Users will get sequential read performance of up to 400 MB/second and sequential write speeds of up to 316 MB/second.

IMMEDIATE PRODUCTIVITY

Problem: Mobile workers often struggle to access applications or IT assets when working in the field or at home.

Solution: The Windows To Go environment's minimal, intuitive interface gets employees working in no time. In addition, IronKey Workspace drives are compatible with virtually every system[1], so users don't have to waste valuable work time hunting down the right host computer.

SALES CONTACTS

WEBSITE
www.ironkey.com

US AND CANADA
securitysales@imation.com
+1 888 435 7682 or +1 408 879 4300

EUROPE
emeasecuritysales@imation.com
+44 (0)1332 597 168

ASIA PACIFIC
apacsecuritysales@imation.com
+65 6499 7199

[1] Any PC certified for use with Windows 7 or higher and some compatible tablet and Mac computers

[2] FIPS 140-2 Level 3 certification #2183

[3] Management is required with the W700SC device

[4] The IronKey flash drive is USB bootable for the Microsoft Windows Enterprise feature "Windows To Go"

IronKey, the mobile security portfolio of Imation Corp.