Device, Data & Document Safeguard Solutions for Government

Business Information Solutions

RICOH
imagine. change.

Digital technologies can enable greater information mobility. Yet security and privacy threats pose great risks. Making information mobile while keeping it secure is critical.

Does This Sound Like Your Current Situation?

Government Departments, Crown Corporations and Agencies process vast quantities of classified, personal, confidential or otherwise sensitive documents. Unfortunately, the risk of unauthorized viewing, theft or abuse of this information is ever present – serious risk and compliance incidents were blamed on ineffective document processes in 76.1% of government and education institutions*. As a result, Government Departments and Crown Corporations must have strong IT Security Risk Management practices to comply with mandated information security regulations.

At risk: Classified, personal, confidential and sensitive information

Digital technology has transformed business by enabling instantaneous data exchange. At the same time, mobile technologies and work-style innovations are changing the way that Government departments and agencies communicate and collaborate. Greater speed and efficiency aren't the only outcomes of these changes – increased security risks can create dangerous vulnerabilities at the device, data and/or document level. Ricoh works with our government clients to help identify gaps in their environment and to put in place a plan to better to safeguard data whether it's in motion (moving through the network), in use (being accessed by end users) or at rest (being managed in short-term or long-term storage).

Your Challenge: Protecting data in motion

Our Solution: Ricoh's Web Image Monitor – an integrated, web-based utility for device management – enables administrators to block or restrict client IP addresses, balance volumes across multiple devices and restrict unauthorized IP addresses from connecting to a print controller. Web Image Monitor also helps prevent theft of user names and passwords, defends against Denial-Of-Service (DOS) attacks and helps prevent viruses from infiltrating unused ports. Ricoh equipment supports secure PDF transmission by scrambling and encrypting data via 128-bit encryption. The sender can establish recipient rights to change or extract content, with recipients using a 32-character password to view the PDF.

Your Challenge: Securing data in use

Our Solution: Ricoh offers effective solutions to help secure data while end users are accessing and working with it. For example, Ricoh's Web Image Monitor provides a centralized audit capability – creating a trail for scanned, faxed (via fax server) and printed information. Ricoh Production Output Solutions enable organizations to analyze print-stream content for Personally Identifiable Information (PII) and replace it with "XXXX." These solutions also encrypt data records in transit for Linemode, Xerox or DJDE/Metacode. Additionally, Ricoh offers functionality to help agencies and departments protect PII, trade secrets and classified information. Administrators can establish policies to block printing of sensitive information and to require watermarks on printed and electronic copies for additional security.

Your Challenge: Safeguarding data at rest

Our Solution: Ricoh offers many features to help safeguard data at rest. Among them: hard-drive encryption to protect against theft, address book encryption to prevent an entire organization from becoming a target of malicious emails, and DataOverwriteSystem Security (DOSS), Ricoh's powerful tool for safeguarding latent images by overwriting them with sequences of 1s and 0s.

*Source- "Its Worse Than you Think", IDC, 2012

Device, Data and Document Safeguard Solutions For Government

PROTECT DATA IN MOTION

Raw Data Streams ▶ Files ▶ Passwords ▶

- 128-Bit Encryption
- Recipient Rights
- SSL/TLS via IPP
- Web Image Monitoring
- Web Address Filtering
- IP Port Disabling

SECURE DATA IN USE

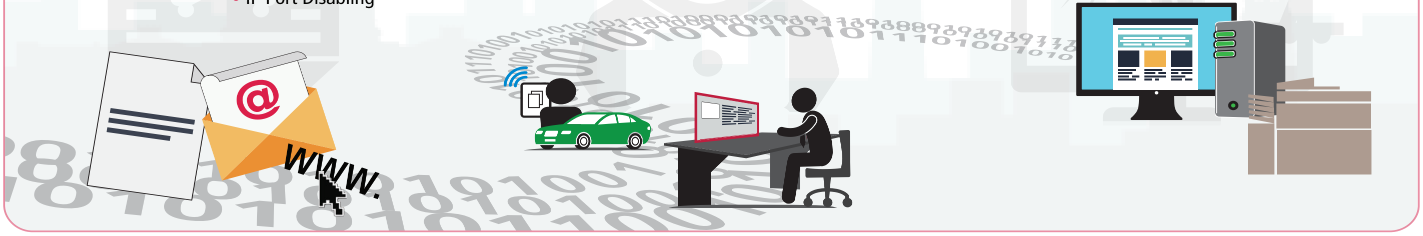
Control Access ▶ Redact Hardcopy ▶ Manage Digital Rights ▶

- Secure Access Card Authentication
- PIN and User ID Protection
- Password Encryption
- Pull Printing
- PII Protection

SAFEGUARD DATA AT REST

Device Storage Protection ▶

- Hard Drive Encryption
- Date Overwrite Security
- Data Wiping



Secure Sockets Layer (SSL)

- To help prevent raw data streams, files and passwords from being intercepted, Ricoh transmits scanned, faxed or printed output over the Secure Sockets Layer (SSL) in the HTTPS protocol. SSL transmission supports compliance with FIPS 140-2, a processing/computer security standard issued by the National Institute of Standards and Technology.

Secure Access Card

- The Secure Access Card is an authentication system that relies on specialized ID cards. After an authorized user inserts a card and enters his/her personal identification number, a request is sent to Active Directory and the user is granted access to appropriate information and output functionality.

Advanced Security Architecture

Ricoh's solution includes the following;

- Ability to pre-flight each device with standardized and predefined security settings before each unit is deployed to each location
- Has Disk overwrite software swiping the Hard Drive as per CSE ITSG 06 standards as a minimum
- Includes Encryption software writing data to the hard drive
- Ability to provide removable Hard Drive functionality for daily removal in secret and top secret installations
- Uses the Trusted Platform Module (TPM) to store keys, signatures and cryptographic functions.
- Option to surrender the HD to the GoC at no additional cost at the end of the lease period and before the machine leaves any of the Federal buildings. Many of Ricoh's MFDs are certified via the IEEE 2600 protection profile which is an information technology security standard developed by the office equipment industry. The standard defines the minimum requirements for security features.

Putting It All Together For You

Federal Departments, Crown Corporations and Agencies must mitigate a host of information security threats. You must also address a range of information security requirements – including compliance to Shared Services Canada, Communications Security Establishment and Treasury Board of Canada standards.

Ricoh Device, Data and Document Safeguard Solutions for Government provide a full complement of security features, functionality and tools to help protect classified, personal, confidential and sensitive information. Ricoh helps make information work for our customers in the Government sector by providing fast and efficient anywhere, anytime access to information while helping to meet mandated information security standards.

RICOH
imagine. change.