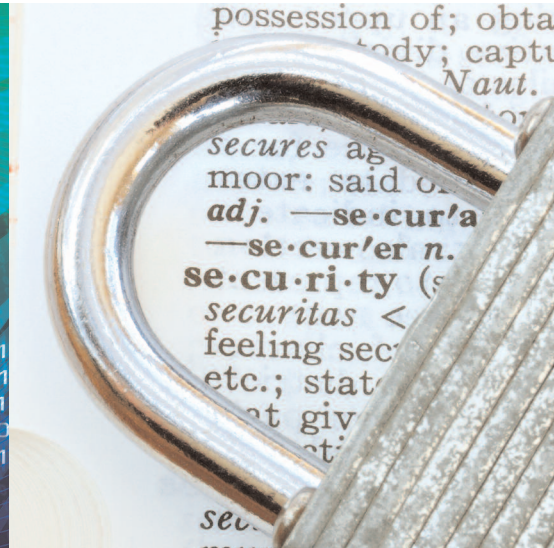


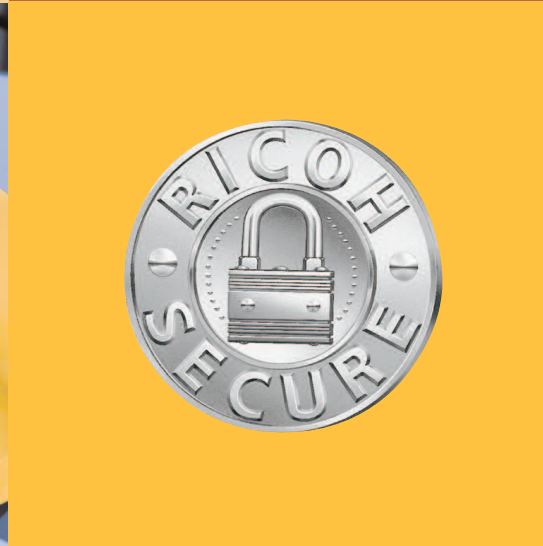
Ricoh Security Solutions  
Comprehensive protection for  
your documents and information

**RICOH**

secure



proven



trusted

# RICOH Security Solutions



**Depend on Ricoh for comprehensive document security. RICOH® understands how vital trust and security are in this digital age. We know it is critical that your documents and data do not fall into the wrong hands. That is why we offer multiple lines of defense to help you protect the information that flows through your Ricoh multifunctional products (MFPs), printers and facsimiles. Our systems feature built-in technologies that offer strong protection for your data. Ricoh also offers a portfolio of optional technologies and professional services that take document and data protection to an entirely new level.**

Whether your Ricoh products are networked or standalone, powerful standard security features guard against breaches while optional security features and services offer a multi-layered approach to provide even greater information protection.



# Secure Trusted Proven Reliable

## Built-In Defense

Ricoh-engineered MFPs and printers are equipped with proprietary software to control machine functions. This standard design feature forms an imposing line of defense against unauthorized users looking to extract documents or data.

- Helps prevent the hard drive from being accessed if it is removed from a Ricoh MFP or printer and connected directly to a PC.
- Destroys File Allocation Tables (FAT) after jobs are finished, making it nearly impossible to locate and retrieve files.

## Automated Protection

Many Ricoh MFPs and printers use Random Access Memory (RAM) instead of a hard drive for document processing. This means that document images are not stored on a hard drive and are not available for retrieval.

- Erases all images automatically when the system is powered down.
- Allows MFPs and printers to be used with confidence — even for jobs involving highly proprietary information.

## Exceptional Network Security

Ricoh offers a range of modern network security solutions that allow you to authenticate users, encrypt network communications and close unused network ports.

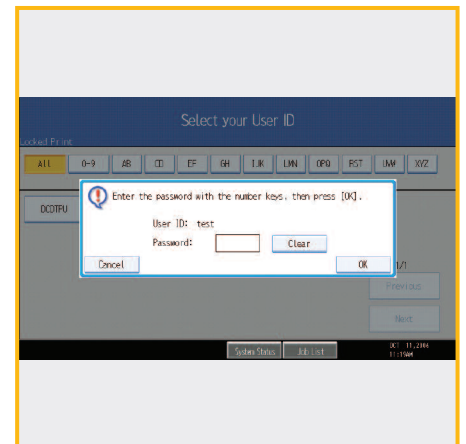
- Helps prevent hackers and other malicious parties from gaining access to networks, servers, output devices and data.
- Helps control access to MFP and printer output (hold for the authenticated user) and restrict access to documents, databases, scanners and other assets.



Proprietary software makes it extremely difficult to access documents and data on a Ricoh MFP or printer hard drive.



Ricoh network security solutions – such as Enhanced Locked Print – protect printed and electronic data against opportunistic or targeted threats, both internal and external.



Enhance document security by configuring Ricoh MFPs to release documents only to authenticated users with a valid user ID and password.

## Automatically Overwrite Data

Ricoh's optional DataOverwriteSecurity System (DOSS) automatically overwrites data from the hard drive after each job is completed — data is destroyed to make recovery virtually impossible.

- Provides two methods for overwriting hard drive data – Event Driven and Overwrite All:
  - Event Driven mode destroys copy, print and scan data immediately after each job is processed.
  - Overwrite All mode overwrites the device's entire hard drive, including stored documents.
- Uses technology based on U.S. Department of Defense (DoD) and National Security Administration (NSA) overwrite methodologies.
- Validated with ISO 15408 Certification to an Evaluation Assurance Level (EAL) of 3 for selected DOSS options<sup>1</sup>.

## Encrypt Valuable Information

In addition to protecting documents and data, you can protect frequently used information — such as address books and administrator or user passwords — with the Ricoh hard drive encryption option.

- Helps keep information typically stored on an MFP or printer from being viewed, even if the electronic data or devices are stolen.
- Encrypts device information rather than destroying it, enabling only authorized users to access the data they need.
- Works in conjunction with the Ricoh DOSS solution for even greater MFP and printer hard drive security.

## Option To Retain Your Hard Drive

When a system is at the end of a lease or ready for trade-in, Ricoh gives you the option to dispatch a certified technician to remove your existing hard drive and give it to you before the device ever leaves your site.

- Ensures that sensitive information is protected with this hard drive surrender option, which provides another level of security and confidence that your documents and data are safe.
- Choose to retain or destroy your hard drive according to your organization's specified security protocols.

<sup>1</sup>DOSS must be installed on the MFP or printer at the customer's location for ISO 15408 compliance.



Ricoh's DataOverwriteSecurity System (DOSS) helps protect your confidential information by automatically overwriting latent digital images on the hard drive after all copy, scan and print jobs.



Guard against data theft – even if the MFP or printer is stolen – with Ricoh's powerful hard drive encryption option.



Select DOSS versions have achieved ISO 15408 certification under limited conditions. ISO 15408 is an international standard for information security that provides verification of IT security features.

# Intelligent Tested Safe Dependable

## Security Solutions Compatibility Chart

	Data Encryption	Document Protection	
	HDD Encryption	DataOverwriteSecurity System (DOSS)	RAM-based Security* (HDD Optional)
<b>Color Multifunction</b>			
Aficio GX3000S			■
Aficio GX3000SF			■
Aficio GX3050SFN			■
Aficio SP C220S			■
Aficio SP C231SF/C232SF			■
Aficio MP C2030			■
Aficio MP C2050/SPF	■	■	
Aficio MP C2550/SPF	■	■	
Aficio MP C2800/SPF	■	■	
Aficio MP C3300/SPF	■	■	
Aficio MP C4000/SPF	■	■	
Aficio MP C5000/SPF	■	■	
Aficio MP C6501/C7501	■	■	
Pro C550EX/C700EX**	■	■	
Pro C900s		■	

	Data Encryption	Document Protection	
	HDD Encryption	DataOverwriteSecurity System (DOSS)	RAM-based Security* (HDD Optional)
<b>Black &amp; White Multifunction</b>			
Aficio SP 1000SF			■
Aficio SP 3400SF/SP 3410SF			■
MP 171F/SPF (copier only)	■	■	■
Aficio MP 1600/SPF			■
Aficio MP 2000/SPF			■
Aficio MP 2500			■
Aficio MP 2500 SPF			■
Aficio MP 2851SP/3351SP	■	■	
Aficio MP 2550B* (copier only)	■	■	■
Aficio 3350B* (copier only)	■	■	■
Aficio MP 3500/4500 SP/SPF/G		■	
Aficio MP 4001SP/MP 5001SP	■	■	
Aficio MP 4000B (copier only)	■	■	■
Aficio MP 5000B (copier only)	■	■	■
Aficio MP 6001/7001/8001/9001	■	■	
Pro 907EX/1107EX/1357EX	■	■	

Note: Additional options may be required in order to achieve full security status.

\* Only available when configured without a hard drive.

\*\* Note: The Pro C550EX/Pro C700EX and Fiery controllers have separate security features.

The security features listed above are for the mainframe GW controller only. If the mainframe is configured with the Fiery, the Fiery's security features take precedence.

	Data Encryption	Document Protection	
	HDD Encryption	DataOverwriteSecurity System (DOSS)	RAM-based Security* (HDD Optional)
<b>Color Printer</b>			
Aficio SP C231N/C232DN			■
Aficio SP C311N/C312DN			■
Aficio SP C420DN	■	■	■
Aficio SP C420DN-KP HotSpot	■	■	
Aficio SP C430DN	■	■	■
Aficio SP C431DN	■	■	
Aficio SP C820DN	■	■	■
Aficio SP C821DN	■	■	
Aficio GX2500			■
Aficio GX e3300N**			■
Aficio GX e3350N**			■
Aficio GX e5500N**			■
Aficio GX7000			■
Pro C550EX/C700EX	■	■	
Pro C900		■	

	Data Encryption	Document Protection	
	HDD Encryption	DataOverwriteSecurity System (DOSS)	RAM-based Security* (HDD Optional)
<b>Black &amp; White Printer</b>			
Aficio SP 4100NL		■	■
Aficio SP 4110N- KP HotSpot		■	
Aficio SP 4210N		■	■
Aficio SP 5100N			■
Aficio SP 6330N	■	■	■
Aficio SP 8200DN	■	■	■
Aficio SP 3400N/SP 3410DN			
Aficio SP 9100DN		■	

\* Only available when configured without a hard drive.

\*\* Note: The GX e3350N/GX e5500N support "IP address filtering" feature only. "Mac address filtering" is not supported. Locked/Secure Print is only available if a Hard Disk is installed.

### Security Solutions Terms

**HDD Encryption:** option that locks data to prevent recovery

**DataOverwriteSecurity System (DOSS):** option that allows you to destroy data to prevent recovery

**RAM Based Security:** select Ricoh systems use volatile RAM instead of a hard drive to process data

# RICOH Security Solutions

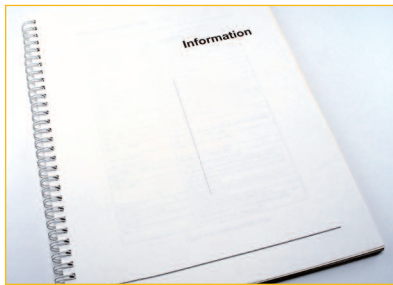
## Security Solutions Compatibility Chart

	Data Encryption		Document Protection	
	HDD Encryption	DataOverwritesSecurity System (DOSS)	RAM-based Security* (HDD Optional)	
<b>Wide Format</b>				
Aficio MP W3600		■		
Aficio MP W5100	■	■		
Aficio MP W7140	■	■		
Epson Stylus® Pro 7700				■
Epson Stylus® Pro 9700				■
FW770				■
FW780				■
Wide Format Color Scanner				■
<b>Digital Duplicator</b>				
Priport DX 3343				■
Priport DX 4542				■
Priport DX 4545				■
Priport DX 3340				■
Priport DX 4640PD				■
Priport HQ 7000				■
Priport HQ 9000				■

\* Only available when configured without a hard drive.

## Supporting documentation and security white papers

Ricoh provides network and device security white papers that detail how information is secured on devices as well as on the network. For ISO 15408 Certified Options and Systems, Ricoh provides Common Criteria Certification Certificates as well as Testing Validation Reports. Customers may use the white papers, the certificates and the reports in their Information Security Plans to demonstrate that reasonable effort has been made to safeguard data and other proprietary assets.



Ricoh supports your organization's information security planning with documentation detailing the security procedures and measures in place for Ricoh MFPs and printers.

**RICOH**  
www.ricoh-usa.com

Bringing Ricoh Value to Your Organization  
Ricoh technology offers a diverse portfolio of solutions to help your organization stay competitive and move ahead. Let Ricoh show you how to empower your business to improve critical processes, increase security and promote environmental sustainability while reducing the total cost of ownership.

Ricoh Americas Corporation, Five Dedrick Place, West Caldwell, NJ 07006  
Ricoh® and the Ricoh Logo are registered trademarks of Ricoh Company, Ltd.  
Epson and Epson Stylus are registered trademarks of Epson. All other trademarks are the property of their respective owners. Print speed may be affected by network, application or PC performance. Specifications and external appearances are subject to change without notice. Products are shown with optional features.

	Data Encryption		Document Protection	
	HDD Encryption	DataOverwritesSecurity System (DOSS)	RAM-based Security* (HDD Optional)	
<b>Facsimile</b>				
Fax1180L				■
Fax2210L				■
Fax3320L				■
Fax4430L*				■
Fax4430NF*				■
Fax5510L*				■
Fax5510NF*				■

\* Ricoh Fax products use volatile RAM for most document processing. Once a job is completed, the RAM is deleted and any image information is destroyed. Select Ricoh Fax systems do have the option of using non-volatile RAM (NV-RAM) for document processing. The non-volatile RAM will store documents until the NV-RAM is deleted. Once the NV-RAM is deleted however, the job data stored is destroyed.