

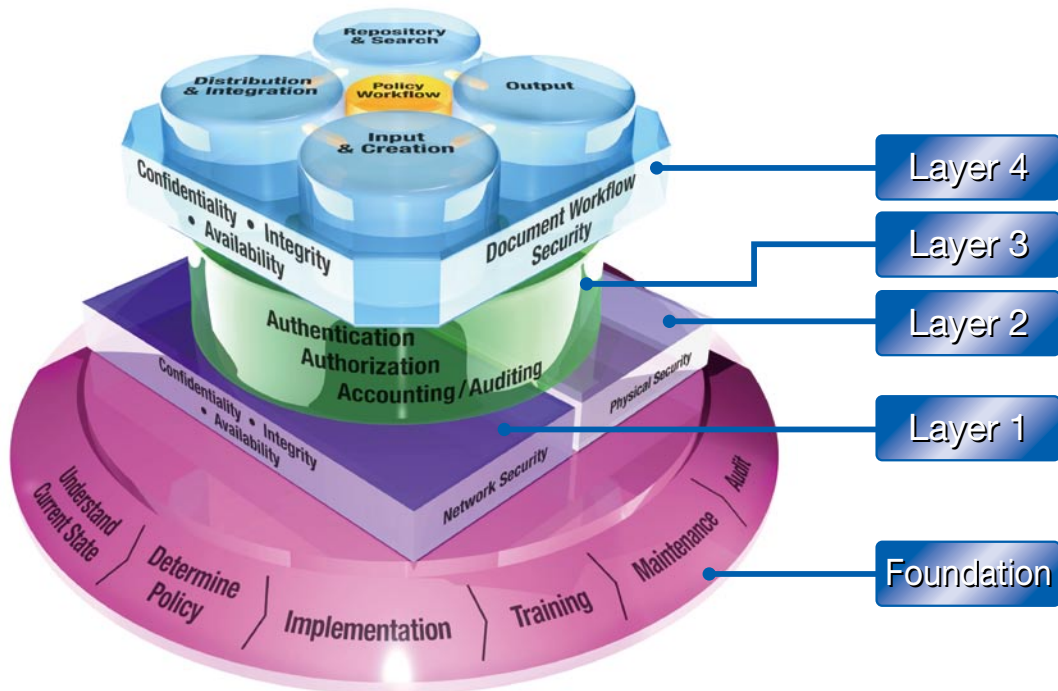
3

Values Ricoh Delivers: Ricoh Document Security

Multilayered Framework Concept Enabling Comprehensive Security

When digital devices are connected to a network, there should be assurance that system resources and data are protected from disruptive forces inside and outside the organization. This assurance enables IT managers to embrace products that would otherwise pose a security risk, while providing employees with high-performance equipment that streamlines the workflow, protects vital business interests, and ensures peace of mind.

Document Security Framework



The Framework Concept

The Document Security Framework concept (Figure 1) is derived from Ricoh's extensive research on our customers' document-related business processes, and reflects respect for the considerable IT investments that have been made. Central to this framework is Ricoh's commitment at each layer, starting with the Physical Security and Network Security Layers (Layers 1 and 2).

These Physical Security and Network Security countermeasures are some of the basic methods used to maintain the Confidentiality, Integrity, and Availability of documents and data.

Once the basic security measures are implemented, stages in the document workflow

must be protected as well. This includes Input & Creation, Output, Repository & Search, and Distribution & Integration (Layer 4). Providing the foundation for this is Layer 3, comprised of Authentication, Authorization, and Accounting/Auditing countermeasures. This AAA Security Layer safeguards the document workflow.

Once the AAA Security Layer is implemented, the document workflow can include correct and safe processes governing information Input & Creation, Output, Repository & Search, and Distribution & Integration. It is then possible to establish proper Document Workflow Security (Layer 4). This can include MFP integration with backend Document Management Systems (DMSs) that provide organizations with the power to control information assets and meet

stringent compliance requirements.

After deploying countermeasures, processes should be reviewed according to the Deming Plan-Do-Check-Act (PDCA) cycle. For example, in the planning stage, it's important to understand the current state of security and define any new policies. To ensure proper use and maintenance of countermeasures, employees must also understand the policies. Furthermore, auditing should be conducted from time to time, in order to check if the security procedures are successful, or if modifications are necessary (Foundation).



Ricoh's Common Sense Approach to Information Security

Keeping the Document Security Framework in mind, Ricoh advocates a multilayered approach to security, one that combines two key objectives: streamlined and efficient workflow, and document security. The goal is to create a controlled system that minimizes risks to information security without unduly impacting document administrators, users or workflow processes.

If the security measures are too costly or complex to roll out, the controls may negatively impact productivity; users may resist.

So, after vulnerabilities and threats to information security are identified, solutions are recommended that:

- Are not overreactions to the perceived risk
- Are non-intrusive
- Are affordable
- Require little or no training

Ricoh Security Solutions

Ricoh digital imaging systems are essentially document portals, on-ramps to the Information Superhighway. As such, these intelligent systems let users tap into information and establish smart processes throughout the organization. Ricoh solutions power the ability to securely scan, route, store, retrieve, and print documents.

While Ricoh is at the forefront of hardware and software development for the office technology industry, equal emphasis is placed on minimizing risks to information security. As a leader in security, Ricoh's world-class security solutions optimize data and document confidentiality and integrity.

The following Ricoh solutions, categorized in Security Layers 1–4 as outlined in The Framework Concept, are designed to help organizations build a secure infrastructure, one that protects physical, network, data, and device assets. Choosing one or more solutions from each category provides multiple layers of security that will help effectively mitigate threats to information security.

Layers 1 and 2: Physical and Network Security

• **DataOverwrite Security System (DOSS)** is a solution that erases data that is temporarily stored on the device's hard drive by automatically writing over the latent image with random sequences of "1's" and "0's," thereby making any effort to access and reconstruct stored files virtually impossible. The DOSS overwrite function can also be activated on demand, for example, to erase a device's entire hard drive after it goes off-lease or when a system is moved from one department to another.

• **HDD Encryption** encodes all data generated on the device using AES 256-bit encryption. A key system is also used so that access to the hard drive is allowed only through that specific device; that is, the hard drive data cannot be accessed if it is placed in a different system.

• **RAM-based Security** is a feature of select devices that when the unit is turned off, data is immediately erased. Though a hard drive is available as an option, there is a security benefit in that latent image data cannot be compromised.

• **Set IP Address Range (IP Filtering)** enables system administrators to restrict authorized connections to the print controller from those hosts whose IP addresses fall into a particular IP range. Commands or jobs sent from unauthorized IP addresses are ignored by the print controller.

• **Network Port Security** offers system administrators the ability to enable or disable IP ports, thus controlling the different network services provided by the print controller to an individual user.

Layer 3: AAA (Authentication/Authorization/Accounting) Security

• **ID Card Authentication** allows authentication workflow to be simplified, to maximize document security and reduce total cost of ownership (TCO) by replacing user name and password input from the device control panel. Instead the user passes his or her ID card through a reader to gain access to device functions. When used with Secure Release, all print jobs are first stored in the device and only released when the job owner's ID card is used. Besides saving time, ID card authentication prevents onlookers from observing PIN entry.

- **User Codes** can be assigned to each user or department, enabling managers to track machine usage by individual code. When this standard feature is activated on the device, a user must enter a valid user code before accessing system functions such as copying and scanning, and so unauthorized use is prevented. Another benefit is reduced TCO.
- **Windows/LDAP Authentication** enables access limitation management by limiting the machine's available functions to specific individuals or groups, thereby protecting the machine settings and data stored in the system from unauthorized access. If the user does not enter a valid user name and password, verified by the Windows server, access to device functions is denied. Ricoh has designed the Windows Authentication capability to use existing Windows user names and passwords, which facilitates seamless integration and eliminates the need to create and remember additional user names and passwords.
- **Job Logs/Access Logs** contain a complete list of every job executed by the device, and are stored in the device. This list may be viewed via Web SmartDeviceMonitor to track device usage by job and/or user. When used in conjunction with external user authentication modes, it will assist in determining which specific users may be misusing a device, or by whom and with which device an unauthorized transmission was sent, to trace the source of leaks.

Layer 4: Document Workflow Security

- **Document Capture** refers to the scanning of hardcopy documents for distribution to other destinations such as an email address, network-shared folder, FTP server, or backend Document Management System (DMS). Scanning is a common way to convert hardcopy into easily shared electronic files. As the cost of managing ever-increasing volumes of paper documents climbs, Web-based solutions that support secure HTTPS communication offer an economical and secure way to streamline the workflow.
- **Enhanced Lock Print** enables all the benefits of a shared, centralized network printing environment by addressing the largest security threat today, the unrestricted access to hardcopy documents in a device's output tray. With Enhanced Lock Print, users store, release, and manage confidential documents with the security of user ID and password authorization. Because this feature is built in, with no extra hardware or software to deal with, it is a fast and simple solution for protecting an organization's confidential and proprietary data, as this prevents others from inspecting or removing output from the tray. An optional card reader offers additional ease of use for environments using existing proximity card systems by providing the automated release of print jobs stored on the MFP.
- **Unauthorized Copy Control** minimizes the risk of unauthorized copying of confidential documents. This feature embeds patterns and text under printed text, eliminating the risk of unauthorized copying of sensitive documents. For example, when a copy is made, an embedded message appears, such as the author's name.
- **Encrypted PDF Transmission** secures transfers of Adobe Acrobat (.pdf) files, which have become the universal standard for creating documents that can easily be

opened and shared by any user on any platform. While Adobe offers a number of security-related features within the Acrobat application to lock and password-protect documents, there is nothing to prevent the files from being intercepted in a decipherable form while traveling over the network. That's where Ricoh's Encrypted PDF Transmission function adds value, as it scrambles and encrypts the data that would otherwise be a transparent document during transmission. And the user password can also be encrypted.

The important thing, as mentioned, is that security measures are implemented that are not too strict or impractical, as this would impede the document workflow. If, for instance, excessive restrictions are placed on print output, office productivity will suffer.

Furthermore, it is essential to take a consistent approach to information security, one that is supported by all levels of management. Indeed, every employee has the responsibility to make reasonable efforts to secure the document workflow. This helps protect information assets throughout the workflow, preventing any individual or group from being the weakest link.

@Remote—Intelligent Remote Management Service for Printing Devices

@Remote enables greater operating efficiency for output devices.

@Remote ("At Remote") is a new kind of Internet-based support for remote management of digital multi-purpose devices and laser printers.

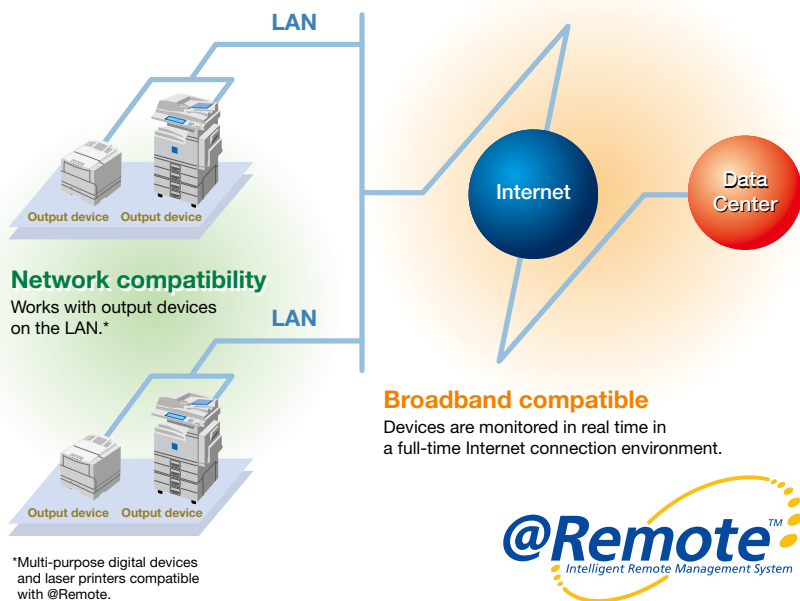
With the advent of this service, the status of networked devices can be monitored in real time, required service can be delivered rapidly, breakdowns prevented, and downtime reduced.

In the event of a breakdown, the troublesome processes of checking the situation and notifying a service center can be eliminated, together with their burden on the user. The automatic meter reading and toner ordering functions also raise the efficiency of day-to-day device management. In addition, the detailed device information for all applicable devices enables more efficient management of the fleet.

This service, one step ahead of the competition, began in Japan at the end of last year. Partial service began in the United States in April 2005, and subsequently will roll out to Europe, Asia and elsewhere.

What is @Remote?

@Remote is a new remote service for networked output devices connected in a LAN/Broadband environment that enables customers to use the devices more conveniently and with greater peace of mind.



Principal Tasks of @Remote

1. Minimize manual tasks

For example, meters and counters of network-connected MFPs and printers are read automatically. Previously, tasks associated with collecting and reporting meter and counter data required the user to check the device and then fill out a postcard or make a telephone call, but this is no longer necessary.

2. Monitor fleet activity

In addition to the total pages printed by each printer, the service reports detailed device use information, such as usage of each paper size, double-sided printing rate, color/monochrome breakdown, and use in the various modes (copying, printing, etc.).

Periodic monitoring of each device on the network keeps track of the connection status and use of each device. That information can

be applied in the management of the devices, and the user can also receive proposals on how to best use the devices, specifically for the environment in which they operate.

3. Automating service call

notification to minimize downtime

A device's self-diagnostic data is automatically forwarded to the Data Center in the event of a breakdown or other problem.

The service provider receiving the information can take immediate and appropriate action, making rapid CE or Service Technician arrangements to simplify the process of requesting a repair, and minimizing device downtime.

Note: The timing of @Remote introduction and the content of the service may vary between countries, regions, installation environments and the devices used. Contact the regional headquarters for your area for details.