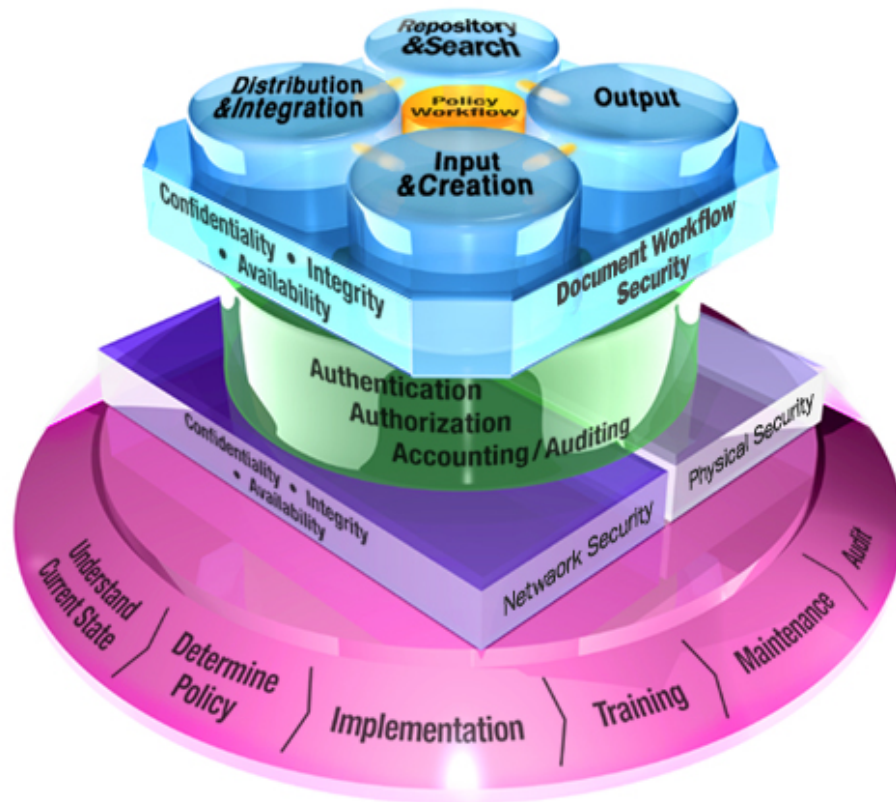


# RICOH

## Information Security White Paper



June 1, 2008  
Version 1.0

**An Overview of the Issues, Concepts,  
and Solutions to Secure Today's  
Digital Document Workflow**

© Copyright 2008 by Ricoh Company, Ltd. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, optical, chemical, manual or otherwise, without the prior written permission of Ricoh Company, Ltd.

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, Ricoh Company, Ltd, its contractors and partners, assume no liability resulting from errors or omissions in this document or from the use of the information contained herein.

Ricoh Company, Ltd reserves the right to make changes in the product design without reservation and without notification to its users.

Any trademarks contained within this document are the sole property of their respective owners.

## Table of Contents

<b>Introduction</b> .....	<b>5</b>
<b>What is Information Security?</b> .....	<b>5</b>
<b>What are Information Assets?</b> .....	<b>6</b>
<b>The Confidentiality • Integrity • Availability Concept</b> .....	<b>6</b>
<b>Vulnerabilities &amp; Threats</b> .....	<b>7</b>
Information at Risk.....	<b>8</b>
Business Sectors at Risk.....	<b>9</b>
<b>Accountability</b> .....	<b>9</b>
<b>The Framework Concept</b> .....	<b>10</b>
<b>Ricoh’s Common Sense Approach to Information Security</b> .....	<b>12</b>
<b>Conclusion</b> .....	<b>12</b>
<b>Appendix</b> .....	<b>13</b>
Ricoh Security Solutions .....	<b>13</b>
Layers 1 & 2: Physical & Network Security .....	<b>13</b>
Layer 3: AAA (Authentication/Authorization/Accounting) Security .....	<b>14</b>
Layer 4: Document Workflow Security .....	<b>14</b>
Federal Mandate Overview .....	<b>15</b>
Security Tips.....	<b>16</b>
About ISO/ IEC 15408 .....	<b>18</b>
<b>About Ricoh</b> .....	<b>18</b>
<b>Glossary of Terms</b> .....	<b>19</b>



## Introduction

---

The purpose of this white paper is to provide guidance on the fundamental issues and concepts of information security, as well as present solutions designed to protect information assets. While this paper is general in nature, those tasked with management of Information Technology (IT) security will gain a better understanding of how to identify and address vulnerabilities that threaten information security. While the type of information that is at risk, and the document workflow itself, are unique to every organization, there is one constant, the need to secure each layer – from document creation through distribution and output.

Central to the document workflow is the network infrastructure and the connected digital office systems – copiers, printers, scanners, facsimile systems, and multifunctional products (MFPs) – that facilitate the generation and sharing of both digital files and paper documents. Today’s sophisticated digital office systems play a vital role in that process.

Having transformed the office landscape, digital technology brings with it new challenges. Specifically, how do you address inherent vulnerabilities that network-connected devices pose? First, assess the vulnerabilities and threats, establish security objectives, and then take appropriate countermeasures. Doing so will mitigate the risk of potentially serious security breaches, and at the same time assist you in meeting strict security compliance requirements.

Whether your organization is comprised of 10 or 10,000 employees, information security should be a top priority. Once that commitment is made, steps can be taken to prevent your business interests from being undermined by inside or outside forces. This is called “risk management,” the principle that assets should be protected through the adoption of appropriate safeguards.

*Note:* For an explanation of acronyms used in this paper, e.g., ISO / IEC, please refer to the *Glossary of Terms*.

## What is Information Security?

---

Information security is the protection of documents that contain sensitive information from targeted or opportunistic threats. Documents are among your most valuable asset (see **Table 1**). The unauthorized collection of confidential, classified or proprietary documents is called industrial or economic espionage, and accounts for annual business losses in the billions of dollars. Whether generated by government, public or private sectors, there is the urgent need to implement effective strategies to protect information assets.

### Organizational Assets

**Table 1**

- |   |   |
|---|---|
| ▪ Physical Assets (e.g., computer hardware, communications facilities, buildings) | ▪ The ability to provide a product or service |
| ▪ Information / Data (e.g., documents, databases)                                 | ▪ People                                      |
| ▪ Software  | ▪ Intangibles (e.g., goodwill, image)         |

*Source: ISO / IEC 13335-1 International Standards, Concepts and models for information and communication technology security management.*

## What are Information Assets?

In this context, information assets refer to documents that contain vital data related to your business. This includes, but is not limited to, client lists, market research reports, patent applications, financial disclosures, and legal correspondence. And since most organizations rely on network environments in order to conduct business, these documents typically exist in both digital and paper form.

Where hardcopy once dominated, information is now stored and managed as data that is easily shared with customers, vendors, clients, and colleagues, perhaps by email, shared folders, Web download, handheld devices, etc. Thanks to increasingly powerful network infrastructures, and widespread access to the Internet, digital information is far more convenient and cost-effective to share and manage. This has dramatically improved workgroup productivity by facilitating collaboration and improving response time to customers, clients, and others. However, this welcome convenience has increased the risk of unauthorized disclosure, transfer, modification, or destruction of information – whether accidental or intentional.

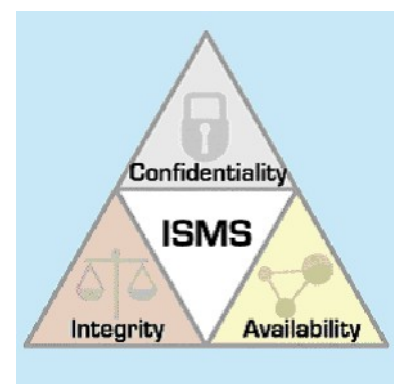
Information technology has become the great enabler for sharing knowledge across your enterprise. However, this advance comes with an imperative: Continually assess information security risks, and then implement safeguards to help prevent theft or loss. Ricoh, as you will learn, has the expertise and resources to assist you in this on-going process.

## The Confidentiality • Integrity • Availability Concept

When we talk about information security, we often refer to Confidentiality, Integrity, and Availability factors. This concept existed before the digital age, but it is even more important today, as the move from analog to digital technology made information far more accessible, and vulnerable.

It is critical that you maintain each factor when establishing internal controls and policies to prevent, deter, and detect security breaches.

- **Confidentiality** – Confidentiality means that the information must only be accessed, used, copied, or disclosed by authorized individuals, and only when and if there is a genuine need.
- **Integrity** – Integrity means that data cannot be created, changed, or deleted without authorization.
- **Availability** – Availability means that the information, computing systems used to process the information, and security controls used to protect the information are all available and functioning correctly when the information is needed.



## Vulnerabilities & Threats

Vulnerability is defined as a weakness of an asset or group of assets that can be exploited by one or more threats. An example of a vulnerability is the lack of access control to a digital imaging device. A threat is defined as a potential cause of an incident that may result in harm to a system or organization. An example of a threat could be the accidental deletion of system or device data or deliberate theft of information assets.

Security measures typically involve the tightening of security to protect against outside threats to a physical building or computer network. However, the greater threat originates from within an organization, those with unrestricted access to digital files and paper documents. So when identifying vulnerabilities and potential threats, first examine network-connected devices for any potential internal security risks.

**Table 2** shows some risks we can find for different information assets, based on the Confidentiality, Integrity, and Availability concept.

**Table 2**

Information Assets		Confidentiality	Integrity	Availability
Information System	Software	<ul style="list-style-type: none"> <li>▪ Unauthorized access</li> </ul>	<ul style="list-style-type: none"> <li>▪ Software bug</li> <li>▪ Operation mistake</li> </ul>	<ul style="list-style-type: none"> <li>▪ System freeze</li> </ul>
	Hardware	<ul style="list-style-type: none"> <li>▪ Theft</li> </ul>	<ul style="list-style-type: none"> <li>▪ Device failure</li> </ul>	<ul style="list-style-type: none"> <li>▪ Theft</li> <li>▪ Destruction</li> <li>▪ End of life</li> <li>▪ Disaster</li> </ul>
Form of Information	Digital Information (Fixed Media)	<ul style="list-style-type: none"> <li>▪ Unauthorized Access</li> <li>▪ Network-based virus</li> </ul>	<ul style="list-style-type: none"> <li>▪ Destruction due to misuse</li> <li>▪ Intentionally falsified</li> </ul>	<ul style="list-style-type: none"> <li>▪ Device malfunction</li> <li>▪ Mistakenly deleted</li> </ul>
	Digital Information (Portable Media)	<ul style="list-style-type: none"> <li>▪ Loss</li> <li>▪ Theft</li> </ul>	<ul style="list-style-type: none"> <li>▪ Destruction due to misuse</li> <li>▪ Intentionally falsified</li> </ul>	<ul style="list-style-type: none"> <li>▪ Loss</li> <li>▪ Accidental or deliberate destruction</li> </ul>
	Paper Information	<ul style="list-style-type: none"> <li>▪ Loss</li> <li>▪ Theft</li> <li>▪ Vulnerable to prying eyes</li> </ul>	<ul style="list-style-type: none"> <li>▪ Forgery</li> <li>▪ Difficult to archive forever</li> </ul>	<ul style="list-style-type: none"> <li>▪ Loss</li> <li>▪ Accidental or deliberate destruction</li> </ul>

In **Table 2**, Information System lists vulnerabilities to information assets in relation to software and hardware. Each category - Confidentiality, Integrity, and Availability - can be compromised if computer-related assets are not protected. For instance, reports of stolen laptops containing unencrypted social security and credit card records can expose people to identify theft. Likewise, malicious virus attacks can undermine network and data security, whether it's a random or targeted event.

The Form of Information category includes Digital Information and Paper Information. Since all organizations generate and disseminate information in both forms, breaches can involve sabotage, theft, or forgery of paper documents, perhaps by a disgruntled employee. Documents can also be lost, accidentally shredded, or deliberately destroyed. Digital files are equally vulnerable as curious employees, or those with ill intent, access sensitive personal information without authorization, for example, medical files, passport records, and financial data. Email records are also at risk of being destroyed, despite internal data-security policies.

The ISO / IEC categorizes threats to information assets as either human or environmental (see **Table 3**). While environmental threats, such as lightning, are outside an organization’s control, human threats are either deliberate or accidental.

**Examples of Potential Threats**

**Table 3**

Human		Environmental
Deliberate	Accidental	
<ul style="list-style-type: none"> <li>▪ Eavesdropping</li> <li>▪ Information modification</li> <li>▪ System hacking</li> <li>▪ Malicious code (virus)</li> <li>▪ Theft</li> </ul>	<ul style="list-style-type: none"> <li>▪ Errors and omissions</li> <li>▪ File deletion</li> <li>▪ Incorrect routing</li> <li>▪ Physical accidents</li> </ul>	<ul style="list-style-type: none"> <li>▪ Earthquake</li> <li>▪ Lightning</li> <li>▪ Flood</li> <li>▪ Fire</li> </ul>

*Source: ISO/IEC 13335-1 International Standards, Concepts and models for information and communication technology security management.*

The impact each type of threat has on an organization is dependent on which asset is targeted. For example, if a computer virus has been unleashed, is it localized to one computer or has the impact been felt enterprise wide. Also, the harm inflicted can be either temporary, or in the case of destruction of an asset, permanent.

During your threat assessment, consider the likelihood of the threat as well as the source. Is the threat an individual or group? Insider or outsider? Is the motivation financial gain or competitive advantage? What is the impact if action is not taken?

▪ **Information at Risk**

In addition to client lists, market research reports, patent applications, financial disclosures, legal correspondence, there are many other types of documents that should not fall into the wrong hands, including:

- Banking/financial statements
- Clinical drug trial data
- Credit card information
- Driver’s license data
- Embargoed press releases
- Exam questions & scores
- Floor plans/blueprints
- Maps
- Medical records
- Mergers and acquisition reports
- New product designs (schematics)
- Personnel reviews
- Social Security numbers
- Travel schedules

This list is only intended to provoke thought, as your organization surely has sensitive documents that are unique. It's also important to note what may be considered a sensitive or confidential document in one environment is not so in another. This is influenced by both the industry sector and corporate culture. Steps taken to secure confidential documents may be voluntarily, perhaps by a business owner or manager, while larger organization and federal agencies must comply with laws governing information privacy.

▪ **Business Sectors at Risk**

A few business sectors that handle at-risk information include the following:

- Federal, state and local government
- Financial services
- Hospitals
- Insurance agencies
- Legal offices
- Medical offices
- Military installations
- Pharmaceutical companies
- Research facilities
- Technology firms

Every enterprise – small to large – must keep high-value, sensitive information, and intellectual property safe, and used in accordance with company policy.

## Accountability

---

A number of Federal mandates require organizations to secure the integrity of certain data, systems, and processes, or be held accountable. In fact, failure to comply with applicable regulations for your industry may have serious consequences, including loss of market share, revenue, and image, as well as possible litigation and fines.

Thus, to open or revisit the topic information security, there are questions you can ask that will uncover needs and potential weaknesses that should be addressed.

1. What are my business' most important information assets?
2. What risks are involved with the creation and distribution of these assets?
3. What steps is my organization taking to improve information security?
4. What are the implications if an information security incident should occur?
5. Do our input/output devices track usage, providing a footprint of each user?

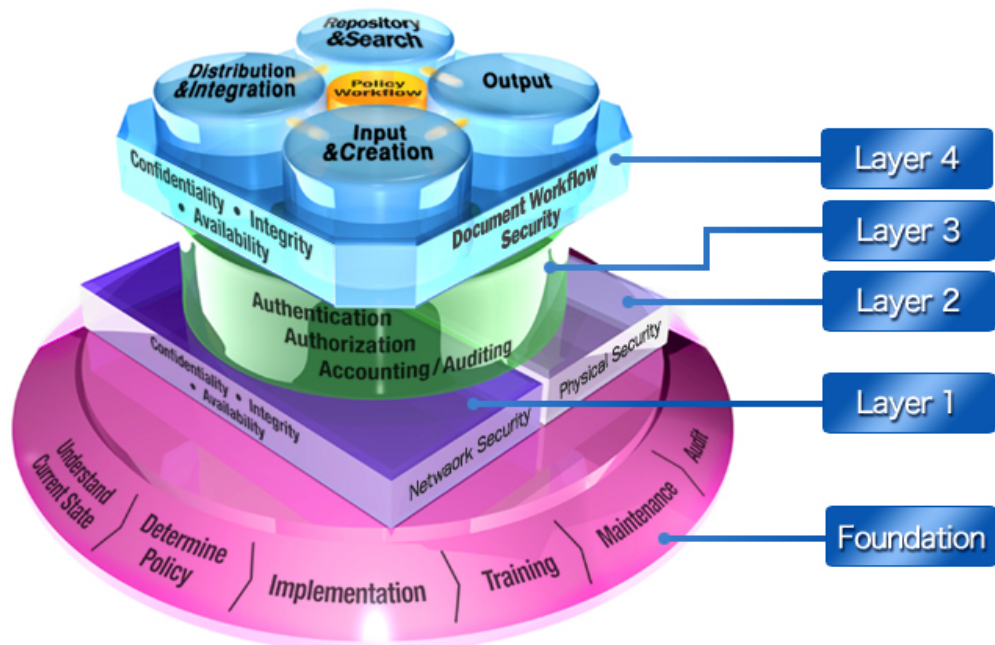
## The Framework Concept

The Document Security Framework concept (illustrated below) is derived from Ricoh’s extensive research into our customers’ document-related business processes, as well as 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 Layer (Layers 1 & 2).

- **Physical Security** refers to countermeasures businesses take to prevent physical break-ins, such as access cards. Credentials embedded on the card validate the employee, vendor, or contractor, allowing access to a building and/or office. Physical security also includes countermeasures used to protect information stored on PCs and MFP devices, e.g., the ability to physically remove the MFP’s hard disk drive.
- **Network Security** refers to countermeasures businesses take to prevent network intrusions, such as firewalls that block unauthorized access to or from a private network. Network security also involves taking measures to close unnecessary ports of network-connected MFPs, or encrypt the communication path between the MFP and remote destination, e.g., network folder, email address(es), etc.

These Physical Security and Network Security countermeasures are just a few basic methods used to maintain document and data Confidentiality, Integrity, and Availability.

### Document Security Framework



Once the basic security measures are implemented, stages in the document workflow must be protected as well. This includes input & creation, output, repository & search, distribution & integration (Layer 4). Layer 4's foundation is comprised of Authentication, Authorization and Accounting/Auditing countermeasures (Layer 3). The AAA Security Layer safeguards the document workflow.

- **Authentication** refers to countermeasures that verify an MFP user's identity, i.e., the user is required to enter a valid user name and password via the MFP's touch screen. These login credentials are compared against a database of authorized users, thus granting or denying access to system functions. Authentication can also be performed using a Smart Card or Proximity Card. To authenticate a device, we can check the Web server certificate when communicating over SSL. Individual documents can also be authenticated.
- **Authorization** refers to the granting a user access to specific MFP functions based on their authentication. For instance, one authenticated MFP user may be granted access to Copy and Fax functions, while another user may Copy, Fax, Scan, and Print functions. A function called Secure Document Release, for example, allows only authorized users to print documents.
- **Accounting/Auditing** refers to the tracking of network resources based on MFP usage. This information can be used for management, planning, billing, or other purposes. For example, Print/Copy Control Software controls user access and monitors print/copy activity on all connected devices, enabling the administrator to pinpoint misuse or abuse.

Once the AAA Security Layer is implemented, the document workflow can include correct and safe processes governing information input & creation, output, repository & search, distribution & integration. It will then be possible to establish proper Document Workflow Security (Layer 4). This can include MFP integration with backend Document Management Systems (DMS) 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's 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 believes you should take a multi-layered approach to security, one that combines two key objectives: streamlined, 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 identifying vulnerabilities and threats to information security, we recommend that you consider solutions that:

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

## Conclusion

---

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

## Appendix

---

### Ricoh Security Solutions

---

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

While Ricoh is on 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 according to Security Layers 1 – 4 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 & 2: Physical and Network Security

- **DataOverwrite Security System (DOSS)** is a solution that erases data that is temporarily stored on the device's hard disk 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. DOSS's 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, i.e., the hard drive data cannot be accessed by placing the drive 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 that latent image data cannot be compromised.
- **Set IP Address Range (IP Filtering)**  
System administrators can restrict authorized connections to the print controller from those hosts whose IP addresses fall into a particular IP range. Commands or jobs sent from non-authorized IP addresses are ignored by the print controller.
- **Network Port Security**  
The system administrator can 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 you to simplify your authentication workflow to maximize document security and reduce TCO by replacing user name and password input from the device control panel. Instead the user swipes their ID card to gain access to device functions. And 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 swiped. Beside saving time, ID card Authentication prevents onlookers from observing PIN entry.
- **User Codes** can be assigned to each end 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, e.g., copying and scanning, prevents unauthorized usage. Another benefit is reduced Total Cost of Ownership (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/password, verified by the Windows server, access to device functions is denied. Ricoh has designed the Windows Authentication capability to utilize existing Windows user names and passwords, which facilitates seamless integration and eliminates the need to create and remember additional user names/passwords.
- **Job Logs/Access Logs**  
A complete listing of every job executed by the device is stored in memory. 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 abusing a device, or whom and which device was used to send an unauthorized transmission to trace the source of leaks.

**Layer 4: Document Workflow Security**

- **Document Capture** refers to the scanning of hardcopy documents for distribution to any number of destinations, perhaps an email address, network-shared folder, FTP server, or backend Document Management System (DMS). Scanning is a popular way to convert hardcopy into easily shared electronic files. As the costs to manage ever-increasing volumes of paper documents climbs, Web-based solutions that support secure HTTPS communication, offer an economical and secure way to streamline workflow.
- **Enhanced Locked Print** allows you to realize all the benefits of a shared, centralized network printing environment by addressing the largest security threat today, the unrestricted access to hardcopy sitting on 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's a fast and simple solution for protecting your 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. What this feature does is embed patterns and text under printed text, eliminating the risk of unauthorized copying of sensitive documents. For example, if copies are made, an embedded message appears, for instance, the author's name.

- **Encrypted PDF Transmission**

Adobe's PDF file format has 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, scrambling and encrypting the data that would otherwise be a very transparent document during transmission. In addition, the user password can also be encrypted.

What's important, as mentioned, is that you implement security measures that are not too strict or impractical, as this will impede document workflow. If you place excessive restrictions on, for instance, print output, office productivity will suffer.

Furthermore, it is critical that you 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. (Also see *Security Tips* for other important ways employees can help support your security initiatives.)

## Federal Mandate Overview

---

There are new and existing federal mandates that impact many organizations, requiring strict compliance. Failure to comply has dire consequences, including hefty fines, possible litigation, eroding customer trust and lost revenue.

- **HIPAA (Health Insurance Portability and Accountability Act)** is a law designed to protect working Americans and their families from discrimination based on pre-existing medical conditions. Securing confidential patient data has thus become paramount for those companies involved in the collection and dissemination of medical records, e.g., hospitals, health care organizations, human resource departments, etc.
- **The Sarbanes-Oxley Act (SOX)** is legislation affecting corporate governance, disclosure, and financial accounting and requires that CEO's, CFO's, independent auditors and committees perform annual evaluations of internal controls and procedures for financial

reporting. To be in compliance, a corporation must document its existing controls that have a bearing on financial reporting, test them for efficacy, and report on gaps and deficiencies.

- **The Gramm-Leach-Bliley Act (GLBA)** is a federal law addressing issues of financial privacy and includes provisions to protect consumers' personal financial information held by financial institutions and governs the collection and disclosure of customers' personal financial information. It also applies to companies, whether or not they are financial institutions, who receive such information.
  
- **The Family Education Rights Privacy Act (FERPA)** is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level.
  
- **Defense Security Service (DSS)** is an agency of the U.S. Department of Defense (DoD). Within areas of DoD responsibility, DSS facilitates personnel security investigations, supervising industrial security, and performing security education and awareness training. DSS verifies that organizations working with classified information do so securely. To verify information is kept secure, an information security plan must be completed. Ricoh has provided information to assist our customers with their information security plans.

### Security Tips

---

Maintaining a safe and secure work environment is critical to maintaining the security of vital information assets. And since every employee handles company information, they are responsible for helping protect the integrity of that information. As such, we offer the following recommendations as part of the Information Security Management System (ISMS) initiative.

#### ▪ Physical Security

---

**Do:**

- Do wear your identification badge at all times.
- Do have visitors, contractors, vendors, and other business partners sign in, wear a badge, and sign out. Remain with these visitors for the duration of their stay.
- Do have contractors and business partners sign a non-disclosure agreement before releasing sensitive information.
- Do report any suspicious activity, report it to your supervisor or security guard.
- Do clear your desk and work areas such that all sensitive information is properly secured.
- Do position your computer screen so unauthorized viewers cannot see the display.
- Do lock all computers, file cabinets, and storage areas when unattended.
- Do pick up and discard (recycle) unused papers.
- Do shred sensitive information when done.
- Do erase the white board after meetings.
- Do check the printer and fax machine after you print or fax to make sure you have collected all hardcopy information.

- Do label documents with their classification level.
- Do keep sensitive documents and electronic media out of sight or locked up when away from your desk or when not in use.
- Do be aware of who is around you when in a public place.

**Don't:**

- Do not prop open exterior doors and leave unattended.
- Do not give your badge or building access card to anyone.
- Do not leave company documents unattended in public places.
- Do not call or fax before double-checking the recipient's phone or fax number.

▪ **Network Computer Security**

---

**Do:**

- Do use a strong password, at least 8 characters in length. Use a combination of letters, numbers, and special characters, e.g., #, %, etc.
- Do change your password frequently or when prompted by the system.
- Do lock your computer (click Ctrl + Alt + Del, then "Lock Computer") when away from your desk.
- Do backup your data regularly.
- Do safeguard all of your data files, whether on a desktop, laptop or USB device.
- Do power down all computer at the end of the day.

**Don't:**

- Do not place a sticky note with your password on the side of your computer.
- Do not share or reveal the method of how the network is accessed, your ID or password.
- Do not install or download software unless approved by the IT department.
- Do not run executable files or attachments of unknown sources.

▪ **Laptop Computer Security**

---

**Do:**

- Do lock access to your computer before leaving the office.
- Do position your laptop so that other parties cannot view it.
- Do avoid storing highly confidential or proprietary information on a laptop.

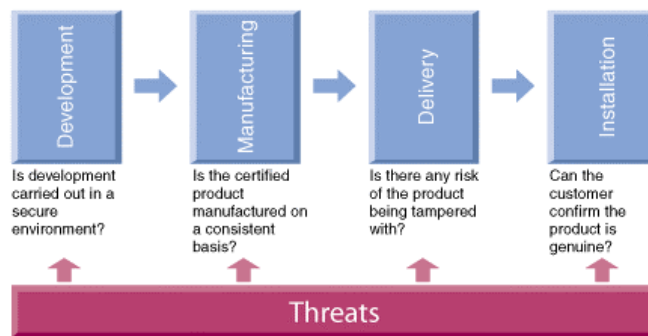
**Don't:**

- Do not leave the laptop unattended when traveling.
- Do not leave the laptop sitting in clear view in the back seat of a car, even if it is in a bag.

## About ISO / IEC 15408

ISO / IEC 15408 is the only international standard for information processing security. This standard helps to determine whether products and systems are properly designed and whether the design is correctly implemented. ISO / IEC 15408 originated from several national standards primarily intended for information systems for defense use. These were unified to become the ISO standard.

The certificate is a testimonial that a product is secure not only in terms of functionality but also in terms of its production processes from product development and design to manufacturing, and its product lifecycle from delivery and installation to use.



To assist our customers with their information security plans, Ricoh has made a commitment to the ISO / IEC 15408 certification process for particular security products and solutions. Ricoh customers may then include the ISO / IEC 15408 certification information obtained by Ricoh in their information security plan. ISO / IEC 15408 certification, when included this way, provides third-party independent verification of security claims. These claims indicate that a reasonable effort has been made to keep information secure.

## About Ricoh

Founded in 1936 in Tokyo, Japan, Ricoh is a global leader in digital office solutions, contributing to the success of businesses in every corner of the world. Our multifunctional printers, fax machines, laser printers and digital cameras set new standards for reliability and innovation. Our current earnings come to over \$17 Billion in annual sales with 83,000 employees and offices in over 150 countries.

## Glossary of Terms

---

**Accountability** – The property that ensures that the actions of an entity may be traced uniquely to the entity. [ISO/IEC 7498-2]

**Authentication** – Authentication verifies the identity of an MFP user by requiring him/her to enter a valid user name and password via the MFP’s touch screen. These login credentials are compared against a database of authorized users, thus granting or denying access to system functions.

**Availability** – The concept that information, the computing systems used to process the information, and security controls used to protect the information are all available and functioning correctly when the information is needed.

**Confidentiality** – The concept that information must only be accessed, used, copied, or disclosed by authorized individuals, and only when and if there is a genuine need.

**Information Assets** – Any documents, in digital or paper form, that contain vital data related to your business.

**Integrity** – The concept of safeguarding documents by preventing unauthorized creation, change or destruction of information assets.

**ISMS** – The Information Security Management System is the effort to identify, control and protect information from unauthorized disclosure.

**ISO / IEC** – International Organization for Standardization and International Electrotechnical Commission. In the field of information technology, the ISO and IEC have established a joint technical committee, ISO/IEC JTC 1, which prepares international standards.

**Risk** – The potential that a given threat will exploit vulnerabilities of information assets, and therefore cause harm to the organization.

**Risk Management** – The principle that assets should be protected through the adoption of appropriate safeguards. Risk management is an on-going activity.

**Safeguard** – A practice, procedure, or mechanism that addresses risk. The term safeguard is synonymous with “control”.

**Threat** – A potential cause of an incident that may result in harm to a system or organization.

**Vulnerability** – A weakness of an asset or group of assets that can be exploited by one or more threats. An example of a vulnerability is lack of access control.

###