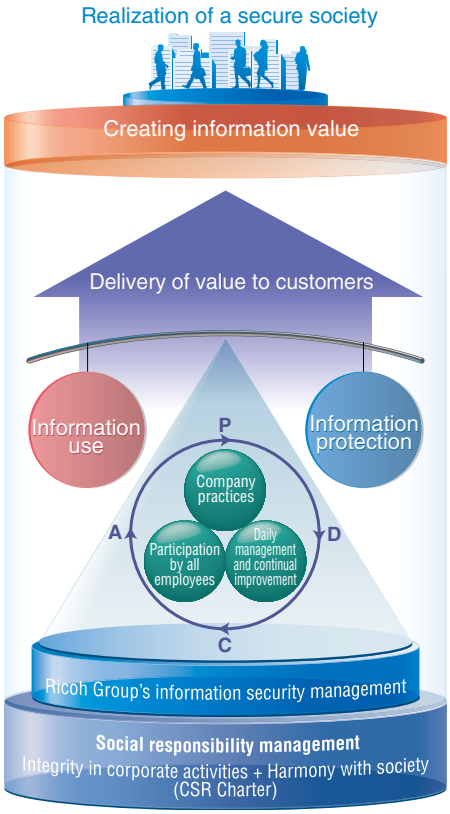
A brand trusted by the information society

In an increasingly complex digital landscape, a crucial factor of Ricoh Group services is to provide tools that our customers can use with complete confidence when it comes to the security of their information.
All our employees are expected to include security in everything they do and to continuously improve security management at their daily worksites. This attitude is ultimately reflected in the security the Ricoh Group provides to customers. The information security built into our products, including MFPs, protects digital and paper-based documents, helping to safeguard the data of our customers.

Information security management

To validate the trust that society places in us, the Ricoh Group involves all its employees in continuous improvement of information security management. Our aim is to balance utility and protection, simplifying the secure use of information by people with legitimate access rights — including business partners — while preventing unauthorized access and leaks.

• The Ricoh Group's information security framework



• ISMS certification mark

ISO27001/IS85241

• ISMS certificate

Reinforcing our information security culture

The primary goal of the Ricoh Group's Information Security Management System (ISMS) is to have all employees engage in proactive, security-conscious behavior as a matter of course, beyond simply following legal requirements or rules. We call this our "information security culture," and reinforce it in three ways: (1) participation by all employees, (2) daily management and continuous improvement, and (3) company practices.

In particular, daily internal use of our products and services becomes in effect a continuous excercise in solving problems related to information security, and allows us to confirm the results of our efforts. The processes we achieve in this way are then passed on to our customers.

ISMS Certification Status

The Ricoh Group obtained uniform ISMS certification (ISO27001) in December 2004. Since then, we have maintained our certification through annual inspections by external organizations and recertification inspections every three years.

As of March 2013, a total of 70 companies — 23 within Japan and 47 overseas — have received ISMS certification.

➤ WEB 1

Information security incidents

In the fiscal year ending March 2013, there were no major incidents that required disclosures to external inspection or audit organizations.

➤ WEB 1 List of Ricoh ISMS registration scope: www.ricoh.com/about/security/management/activity/index.html

Security in products and services: MFPs

In MFPs, the Ricoh Group was among the first to introduce measures to prevent leaks of digital and paper-based documents or falsification of data.

We consider all possible threats that may arise during the lifecycle of a digital or paper-based document — from the creation of a document through its processing, storage, preservation and disposal — and develop and deliver the functions necessary to protect the document from those threats.

For further security and to allow customers to use Ricoh products with greater peace of mind, we obtained international certification standards for a wide range of products, including the ISO/IEC 15408 security function certification backed by an objective third party, Common Criteria (CC).

The Ricoh Group will continue to safeguard the information assets of our customers with products adapted to their specific office environment and security policies. We will also issue reports on information security on a regular basis and support our customers in implementing security controls.

Security around MFP products

As the information society has grown, we have become increasingly exposed to a variety of new threats such as computer viruses, leaks of personal information, and unauthorized access to data. Devising measures to counter these threats is now an imperative part of doing business.

These security threats are not limited to computers, servers and networks, so it is essential to set up and operate MFPs correctly. As one of the first to focus on security measures for MFPs, we have thoroughly considered all types of potential security breaches. ➤ WEB 2

Obtaining Common Criteria certification

To confirm the effectiveness of our security functions, we applied for Common Criteria certification of international security function standards (IEEE 2600.1), and in February 2010 we became the world's first organization to obtain IEEE 2600.1 for an MFP, the imagio MP 5000 SP/4000 SP (launched in February 2008). Since then, we have developed a broad line of CC-certified products so that our customers can be assured that their information is safe.

• Security threats in offices

Unauthorized access via networks

Unauthorized access via telephone lines

Tapping and alteration of information over the network

Unauthorized access via the device's operator panel

Information leaks from storage media

Information leaks via hard copies

Information leaks due to carelessness

Hard disk security functions

Hard disk drive (HDD) encryption

Address books, authentication information and accumulated documents stored in multifunction copiers are encrypted as they are stored. This function prevents information from being leaked even if the hard disk drive is physically removed.

Data Overwrite Security System

When a document is scanned by an MFP or scanner, or when data is received from a computer, some data may be stored on the hard disk drive or memory device — for example, temporary image data, data the user has chosen to save, or device configuration data. When such data is no longer needed, this function erases the data by over-writing it.

Encryption key protection via TPM (Trusted Platform Module)

TPM is a tamper-proof hardware security module that performs cryptographic functions and securely stores cryptographic data. Ricoh uses the TPM to store the root encryption key that protects the hard disk data encryption key and the digital certificate of the MFP, and to perform a trusted boot operation that validates MFP firmware authenticity before permitting the MFP to operate. The root key and cryptographic functions are always contained within the TPM and cannot be altered from outside. This provides high-level assurance of the validity of the MFP's firmware, device identity and hard disk security.

CC: Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)

Common Criteria is an international standard for information security that provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and repeatable manner. Customers can use CC to confirm that a product meets their security requirments and compare security specifications across different products.

➤ WEB 2 Security Threats and Countermeasures: www.ricoh.com/about/security/products/mfp/countermeasure/