Protection of Data on the MFD and Printer

RICOH
imagine. change.

Ricoh Proprietary Software System Overview

Ricoh-designed multifunction device and printer products include technology designed to help prevent the hard drive from being accessed even if the hard drive is removed from the device and connected to a PC. Ricoh products use proprietary software to process data, which makes accessing hard drive information extremely difficult.

RAM Based Security Overview

Select Ricoh MFD (Multifunctional Devices) and Printer systems use RAM (Random Access Memory) instead of a hard disk drive for document processing tasks as a copier and basic printer (a hard drive may be available as an option for some models). The security benefit to the non- hard drive configuration is that information processed with RAM is volatile (i.e. when the system is turned off, data is immediately erased). Without a means to permanently store data, such as a hard drive, the security threat posed by illicit access to the system's hard drive is eliminated.

These RAM-Based MFD and Printer systems may be used for environments where information security is the top priority.

DataOverwriteSecurity System Overview

To provide enhanced security for our MFDs and Printers, Ricoh offers the DataOverwriteSecurity System (DOSS) for select systems. DOSS offers two processes for overwriting the hard drive data, "Event Driven" and "Overwrite All".

EVENT DRIVEN:

- DOSS overwrites the sector of the hard drive used for data processing after the completion of each job. During the overwrite process, the data is destroyed to preclude illicit recovery.

OVERWRITE ALL:

- DOSS can also offer the capability to overwrite the entire hard drive up to nine times. Overwriting the entire hard drive is designed to destroy all data at the end of the system's useful life or when being returned at the end of a lease.

The DOSS can be included at the time of initial installation or at any point during the life of the system.

To verify that DOSS functions appropriately and securely, Ricoh has obtained DOSS ISO 15408 certification for many versions. This certification provides independent third party verification of DOSS operating characteristics. ISO 15408 certification is accepted by various governments and may be used as a proof source for customers' information security plans.

DOSS Hard Drive overwriting can be chosen from following three methodologies:

U.S. NATIONAL SECURITY AGENCY (NSA) METHODOLOGY:

- Overwrite twice with random numbers
- Overwrite once with Null (0)

DEPARTMENT OF DEFENSE (DoD) METHODOLOGY:

- Overwrite once with fixed numbers.
- Overwrite once with complement of above fixed numbers.
- Overwrite once with random numbers.
- Carry out final verification

RANDOM NUMBERS METHODOLOGY:

- This method overwrites data a specified number of times (from one to nine times) with random numbers.

Hard Drive Encryption Option Overview

The Hard Drive Encryption for Ricoh MFDs and Printers provides security for information that needs to be stored on the MFD or Printer and reused again. Examples of information that may need to be stored for reuse include administrator and user passwords and address book information.

Data encryption is compatible with the three memory storage areas on the MFD or Printer, (the Hard Drive, Non Volatile RAM, and flash ROM memories.)

The use of the Encryption feature makes it possible to prevent data from being viewed, even in the event that the encrypted data was stolen. The encryption applies to active data (data still in use), as well as data from completed copy and print jobs (latent data) even if over written by DOSS.

The encryption level for the hard drive is to the Advance Encryption Standard (AES); up to 256 bits for select newer models.

The Hard Drive Encryption encrypts certain data so only authorised users may access the information. DOSS destroys data so it cannot be reused. The Hard Drive Encryption and DOSS may be used in conjunction and will not interfere with MFD or Printer operations.

Locked Print Overview

Locked Print (password-protected print) helps maintain confidentiality by suspending document printing until the authorised user (author/creator) enters the correct PIN (Personal Identification Number) from the device control panel. This reduces the possibility of an unauthorised person viewing or removing a document from the paper tray. (Locked Print requires a hard drive that may be optional, depending on model.)

Enhanced Locked Print Overview

Enhanced Locked Print lets you capture all the benefits of shared, centralised MFDs while still promoting good document security practices. Users store, release and manage confidential documents with the security of user ID and password authorisation. It's one fast and simple solution for helping protecting your organisation's confidential and proprietary data.

Users can send documents to printers where they are securely held until released by the authorised user.

Documents cannot be picked up at the printer by another user, protecting information confidentiality.

Documents stored at the printer are encrypted.

Enhanced Locked Print is installed to the Multifunctional-printing device either via embedded firmware (SD Card) or remotely via Web Interface.

Administrators and users can configure Enhanced Locked Print through a simple web browser-based interface.