Protection of Data on the MFP and Printer

- **Ricoh Proprietary Software System Overview**
  - Ricoh-designed MFP 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 MFP 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 MFP and Printer systems may be used for environments where information security is the top priority.
- **DataOverwriteSecurity System Overview**
  - To provide enhanced security for our MFPs 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 option 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 the U.S. Government and may be used as a proof source for customers' information security plans. Currently, Ricoh has ISO 15408 Certification to an Evaluation Assurance Level (EAL) of 3 for the following DOSS versions:
    - DOSS Type C
    - DOSS Type D
    - DOSS Type F
    - DOSS Type I
    - DOSS Type H

  - **DOSS Hard Drive overwriting can be chosen from following three methodologies**
    - **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 Option for Ricoh MFPs and Printers provides security for information that needs to be stored on the MFP 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 MFP or Printer, (the Hard Drive, Non Volatile RAM, and flash ROM memories.) The use of the Encryption Option 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 Option encrypts certain data so only authorized users may access the information. DOSS destroys data so it cannot be reused. The Hard Drive Encryption Option and DOSS may be used in conjunction and will not interfere with MFP or Printer operations.
- **Removable Hard Drive Option Overview**
    - Convenient and easy to use, Ricoh's Removable Hard Drive Systems secures the MFP's internal hard drive within an external rigid housing device that utilizes a key lock system. A numbered labeling system ensures the Removable Hard Drive is easy to identify while in storage or when being replaced in the system. Also provided is a cushioned static-free case to protect the Removable Hard Drive while in transit or storage.
    - To provide even more security and flexibility when dealing with both classified and non-classified documents, an optional additional Removable Hard Drive is also available. This allows Ricoh MFP's to handle two separate interchangeable Removable Hard Drives;
        - **One RHD for classified documents**
            - After the classified documents have been copied or printed, the classified drive can be removed and placed in a secure location
        - **One RHD for unclassified documents**
            - Unclassified drive can be reinserted for unclassified copying or printing.
    - The Removable Hard Drive is placed in a strategically accessible area for easy authorized removal and storage.
    - Enhances security by allowing the physical separation of data from the input/output device, preventing access to remnant data.
    - Removable Hard Drive-enabled Ricoh systems operate seamlessly with the device's robust copy, print and scan features.
    - Operates in conjunction with Ricoh's DataOverwriteSecurity System, providing a multi-layered approach to securing sensitive documents.
    - All functions are available (copy, print, scan, fax and document server) when the Removable Hard Drive is installed. Select models will not support the Hard Drive Encryption and Fax Option when enabled with a Removable Hard Drive Option.

- **Hard Drive Surrender Option Overview**
  - The Ricoh Hard Drive Surrender Option is designed for customers that wish to retain complete control of the information contained on their hard drives. When an MFP or Printer has reached the end of its lease or is ready for trade-in, Ricoh gives you the option to dispatch a certified technician to remove the hard drive from the Ricoh MFP and/or Printer and give the customer custody of the hard drive before the equipment is removed from your site. Of course, where the equipment must be returned to Ricoh or a leasing company in good working order, there is an additional small cost to install a new hard drive. The customer is then able to dispose of the hard drive containing their information as they choose.
  - This option is also available for MFP and Printer products that are not supported by DOSS or the Hard Drive Encryption Options.
- **Locked Print Overview**
  - Locked Print (available through Ricoh's advanced print drivers) helps maintain confidentiality by suspending document printing until the authorized user (author/creator) enters the correct PIN (Personal Identification Number) from the device control panel. This reduces the possibility of an unauthorized 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, centralized MFPs while still promoting good document security practices. Users store, release and manage confidential documents with the security of user ID and password authorization. It's one fast and simple solution for helping protecting your organization's confidential and proprietary data.
  - Users can send documents to printers where they are securely held until released by the authorized 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.