RICOH

April 29, 2010

Ricoh Technology Security Information

Ricoh understands the importance of data security. We also recognize that every customer environment is unique, and that each customer must make its own risk assessment and determinations regarding security, data retention, data privacy and confidentiality compliance.

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

Since 2002, Ricoh has offered additional enhanced MFP and printer security options and features. Below is an overview of the options available to customers who identify concerns related to MFP hard drive security during the service life and/or at the time of return:

DataOverwriteSecurity System (DOSS) Option
To provide enhanced security for our MFPs and printers, Ricoh offers the DataOverwriteSecurity System (DOSS) for its MFP and printer products. 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 prevent recovery. Additionally, DOSS also offers the option of overwriting the entire hard drive up to eight times. This feature may be used at the end of the lease or if the MFP or printer is moved to another department. Overwriting the entire hard drive takes a few hours and may be added before or after the initial sale.

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 operations. ISO 15408 certification is accredited by the U.S. Government and may be used as a proof source for 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

Hard Drive Encryption Option
The Hard Drive Encryption Option 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 books. The Hard Drive Encryption Option differs from DOSS in that the information encrypted is not destroyed, but locked up 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 operation.

Network Security Features
Ricoh offers a wide range of network security features such as user authentication, network communication encryption and the ability to close unused network ports. These features are used to secure Ricoh devices on customer networks.

Additional detailed information regarding Ricoh's security offerings is available on http://ricoh-usa.com/products/security.