



Equipment Security

Equipment Hard Drive Protection

Once data has been written to any disk drive, the potential exists for it to be retrieved—even *after deletion*—unless it's been effectively overwritten or destroyed. Temporary or stored data could be accessed on your copier during your business' use of the device, or after the device is returned, recycled or resold.

Thermocopy utilizes a standard procedure for processing equipment that has been used by our customers. We also offer security products that can erase data, encrypt data, or a combination of both functions. These measures make it very difficult—or impossible (depending on the specific product and options)—for hackers to retrieve data through disk utilities or file recovery tools.

Thermocopy also offers our customers the option to have the hard drive physically removed from used equipment and shredded—or returned, to keep or destroy as you choose. A new hard drive would be installed in any used equipment to be resold to another user.

Our Standard Procedures

The standard procedures described below are free of charge to our customers and provide the most basic of equipment security. Our certified technicians will perform these security steps and all processes will be verified and tracked. Your Thermocopy representative can advise you on which additional options may be needed, depending on your devices and the level of security required.

✔ All **RICOH, KYOCERA** and **CANON** equipment containing a hard drive that is to be resold or returned to leasing will be subject to security procedures to delete user data on the system and hard drive. These security measures will be provided at no additional cost to our customers.

✔ Our manufacturer-certified Thermocopy technicians may delete data to include, but not limited to:

- IP Addresses
- Network Data
- Email/Fax Addresses
- User Settings
- Company Directories
- Contact Lists
- Job Logs

✔ **RICOH** and **KYOCERA** equipment will have the hard drive formatted utilizing the manufacturer's utility contained within the device. RAM memory will be cleared of all user-specific settings, which varies somewhat based on the actual model.

✔ **CANON** equipment containing a hard drive will be overwritten utilizing the HDD Format Feature. The data that this procedure overwrites includes contacts from the address book, data in all mailboxes, data in Advanced boxes for the imageRUNNER Advanced, and all other customer data and settings.

✔ Equipment returned to Thermocopy's warehouse will be recorded each day by our logistics team and placed in a "holding pattern" until such time that the disposition is determined, *i.e.* lease return, wholesale, disposal, returned to stock. All returned equipment is logged each day and these records are maintained indefinitely.

Our Standard Procedures (cont.)

✔ All returned equipment will be secured in Thermocopy's warehouse facilities until a certified technician performs specific data deletion procedures on the device and completes a Data Deletion Certificate.

✔ A member of our logistics team will verify that the data deletion procedure has been accomplished before shrink wrapping, labeling and placing the equipment in the appropriate location.

✔ All equipment utilized for parts or recycling will have the hard drive removed.

Additional Security Options

The best protection against unwanted access to the confidential or sensitive information contained in your documents is to implement a **proactive security strategy**. Thermocopy offers our customers a variety of options for hard disk drive data security for every brand we carry.

You can trust Thermocopy to secure your hard disk drives—our company has experience installing and implementing certified security products for many customers who deal in sensitive information, such as medical and legal records, as well as our government agency clients who require the very highest levels of irretrievable encryption and data destruction.

The following options are offered at an additional charge. All systems and kits are device specific. Your Thermocopy representative can check for compatibility with your equipment and provide more detailed information.

Please contact us to discuss specific concerns you may have for your equipment security. Our consultants can customize a security package for your business based on your devices and security requirements.

RICOH

Data Overwrite Security System (DOSS)

DOSS destroys data / ISO 15408 Certification to Evaluation Assurance Level 3 (EAL3)

- DOSS Type C
- DOSS Type D
- DOSS Type F
- DOSS Type I
- DOSS Type H

Hard Drive Encryption Option

*Encrypts data, but does **not** destroy data.*

CANON

HDD Data Erase

Meets Common Criteria Certification of Evaluation Assurance Level 3 (EAL3)

HDD Data Encryption Kits

- MFP Security Chip 1.00

Meets Common Criteria Certification of Evaluation Assurance Level 3 (EAL3)

Separate Function Kits

- Data Erase Kit A – Does **not** meet EAL3
- Data Erase Kit B – Does meet EAL3
- Data Encryption Kit B – Does meet EAL3

Combined Function Kits (Overwriting and Encryption)

- Security Kit A – Does **not** meet EAL3
- Security Kit B – Does meet EAL3

KYOCERA

- Data Security Kit B – Data Destruction*
- Data Security Kit C – Data Destruction and Encryption*
- Data Security Kit D – Data Destruction*

** ISO 15408 Certified*

- Data Security Kit E – Data Destruction and Encryption
Undergoing evaluation for ISO 15408 Certification (4/10)