

Security of Hard Disk Drive-based imageRUNNER Devices

Is there a potential concern regarding Canon Hard Disk Drive Security?

There has been recent national news coverage referencing a concern for the data security of copiers/multifunction devices with hard drive storage. Canon U.S.A., Inc. has been aware of these security concerns prior to the recent news coverage and has offered a security strategy that implements both standard and optional measures across the imageRUNNER line to mitigate these risks.

We would like to clarify the standard and optional security features and provisions included on Canon imageRUNNER technology designed to reduce the risk of data or information leakage.

All Canon imageRUNNER devices equipped with HDD have standard features in place to protect the information on their internal hard drive image servers and prevent the misuse or theft of the stored data. The image data from routine job processing during copying, printing, scanning and faxing is temporarily written to the HDD in a proprietary Canon file format. This file format is not compatible with file systems commonly used and not useful outside of the imageRUNNER device. The HDD directory information is also stored on a separate system board, making file reconstruction infeasible in the event the HDD was removed. Furthermore, all temporary and permanent data written to the hard drive is written in random, non-contiguous locations on the hard disk drive. The compressed data can, in turn, only be read by an imageRUNNER device using the proprietary format, which is integral to the operating system of the device, making the stored data highly secure.



Hard Disk Drive Format is another security feature standard on all imageRUNNER devices that, when activated by a system administrator, ensures the imageRUNNER device's hard drive is wiped clean before returning it off lease, redeploying a device in another location, or disposing of a unit. This feature is designed to accommodate your company's security policies and eliminate customer concern with company data remaining on an imageRUNNER hard

drive at end of product lifecycle.

Canon offers optional Security Kits for the imageRUNNER devices, designed for those users and companies requiring enhanced security of document data stored on the Hard Disk Drives. The imageRUNNERs devices can be configured with security kits that offer both overwrite and encryption technology. The overwrite technology can overwrite the internal hard disks up to three times, while the data on the hard drive may be encrypted with 168 bit technology causing the data to be unreadable.

Recently, the Canon imageRUNNER Security Kit received five stars, the highest possible rating, from Buyers Laboratory Inc. in a recently published evaluation report. The full report, entitled *Canon imageRUNNER Security Kit*, is available for subscribers on Buyers Lab Inc. website, www.buyerslab.com . For additional information on the security features available for the Canon imageRUNNER Series, please consult the *Canon Security Solutions for the imageRUNNER Series and imagePlatform Devices* brochure available on ISG Central <http://isgcentral.cusa.canon.com/> .