

### Safeguard Your Corporate Information

#### Information is a Company's Most Important Asset—Protect it!

It is often said that information is the most important asset of any business. This has never been truer than today, when companies and individuals are inundated with data making its migration to becoming valuable information.

Due to the vital nature of corporate information, safeguarding it has never been more important. Canon recognizes this important need and, as a result, has developed comprehensive security capabilities across our entire imageRUNNER product line.

#### It's Just a Copier...Who Needs Security?

The marketplace has evolved over the last several years and so has the technology associated with office equipment. Traditional office equipment has gained major strides in technology, expanding its functional capabilities while, at the same time, becoming an integrated part of the corporate network and the Internet. The result is that a new level of security is required.

As the marketplace rapidly transitions from the purchase of traditional stand-alone copying, printing, faxing, and scanning products to devices

that integrate these functions and link them to corporate networks, a whole new era in information management has begun. Securing these systems is now an important aspect of an overall network and information security strategy.

#### The Solution

Canon's attention to emerging market trends and the details surrounding customer security requirements has driven the development of imageRUNNER product features that are designed to thwart data loss and the potential threats posed by hackers.

Based on the most stringent government agency requirements, Canon's security capabilities fall into three key areas. These include standard device security, network and print security, and data overwrite protection.



Mail Boxes.

#### Standard Device Security

All Canon imageRUNNER products ship with many security features as standard offerings. When shipped in their base configuration, as stand-alone digital copying devices, the imageRUNNER product line offers the following protection:

**Copy Control Access:** An embedded feature in all imageRUNNER devices, Copy Control Access permits device administrators to register up to 300\* department and user IDs, thereby requiring end-users to enter a password prior to accessing device-copying capabilities.

**Restricting Device Setup Screens:** A standard feature, imageRUNNER device setup screens can be password-protected to ensure that administrative device settings are not changed without appropriate authority.

**Mail Box Password Protection:** Each imageRUNNER product ships standard with up to 100 User Mail Boxes. These Mail Boxes can be used for storage of scanned and printed data, integrating scanned and printed data, or long-term document storage. Mail Box security is provided through the ability to lock down access to the Mail Box system via system administrative passwords, and the ability to designate unique passwords for access of individual device

#### Network and Print Security

When implemented in networked configurations, Canon imageRUNNER products offer unique benefits as communication hubs for corporate information. Network connectivity also brings heightened requirements for security. As a standard offering, Canon imageRUNNER products deliver the following network and print security capabilities:

**Enabling/Disabling Protocols:** Through Canon's system setup and installation utilities, network administrators are provided with the ability to enable or disable specific device protocols and print applications. As a result, unwanted device communication can be disabled, as can access to the system via specific transport protocols.

\* Total number of IDs depends on model. Please consult your Canon-authorized Dealer for further details.

Keeping Your Secure Data Safe

Keeping Your Secure Data Safe

**Print Job Accounting:** A standard feature in Canon's printer drivers, Print Job Accounting requires users to enter an administrator-defined password prior to printing, thereby restricting device access to those authorized to print.

**Secured Print:\*\*** A standard capability, the Secured Print function within Canon's printer driver requires an end-user to enter a password prior to job release. Upon receipt of the print job at the device, the user must enter the job password in order to print. Using this feature, users can ensure that they are at the device when their job is delivered.

**Mail Box Printing:** Another secure document delivery feature is Mail Box Printing, which allows users to send a job to their individual Mail Box. Once stored in the Mail Box (if it is password-protected), a user must enter his or her password to retrieve jobs previously stored.

### Data Overwrite Protection

Many of the functional capabilities and unique features of Canon imageRUNNER technology are delivered through the use of an internal Image Server. The Image Server used within Canon imageRUNNER products is comprised of hard disk storage and RAM, and varies in size from device to device. Although storage and RAM size vary, the internal Image Server delivers consistent functional capabilities from one imageRUNNER system to the next, and is largely responsible for data handling across all device functions.



Because of its architecture, the vast majority of jobs processed by imageRUNNER systems results in images being written to the Image Server hard disk drive and RAM. Following the completion of jobs, latent image data remains on the Image Server hard disk.

To address this particular condition, Canon has developed an optional imageRUNNER Security Kit. With the imageRUNNER Security Kit, security-conscious customers can configure their imageRUNNER systems with the internal software necessary to randomly overwrite internal Image Server hard disks, erasing previous data stored as part of routine job-processing tasks.

The imageRUNNER Security Kit offers a number of administrative options, permitting system administrators to set varying levels of overwrite protection (see Canon Security White Paper for further details). When combined with the standard security protection offered on base product and networked device implementations, the imageRUNNER Security Kit delivers the ultimate Canon solution for information protection.

### It's all in the Details



There are many details associated with Canon's imageRUNNER security initiatives. To access additional information on Canon's capabilities in this area, a detailed imageRUNNER Security White Paper can be found on Canon's website at [www.usa.canon.com](http://www.usa.canon.com) or [www.imagerunner.com](http://www.imagerunner.com).

The security requirements associated with information management will continue to evolve, placing greater demands on customers and suppliers alike. Canon is committed to meeting these new challenges, and continuing to deliver solutions that address the needs of our customers while simultaneously providing the greatest level of protection for corporate information.

**Canon** KNOW HOW™

1-800-OK-CANON  
[www.usa.canon.com](http://www.usa.canon.com)

Canon U.S.A., Inc.  
One Canon Plaza  
Lake Success, NY 11042

\*\* Includes imageRUNNER 2200/2800/3300/3300i/5000/6000/7200/85/8500/105 models.

Canon is a registered trademark, and IMAGERUNNER and Canon Know How are trademarks of Canon Inc. IMAGEANYWARE is a service mark of Canon U.S.A., Inc. All other terms and product names may be trademarks or registered trademarks of their respective owners, and are hereby acknowledged.

Specifications are subject to change without notice.

