Precautions to Take when Erasing Data Prior to Disposing of or Returning an MFP

Introduction

When you dispose of or return an MFP, it is important to erase all the data in the machine, such as that on the hard disk and memory. To prevent the leakage of sensitive information, be sure to erase the data yourself.

It has been reported that there is a risk of data leakage through the use of special software that recovers data remnants on a hard disk.

For this reason you should read this manual carefully and take appropriate measures. It is up to you to protect your information assets.

The manufacturer is not responsible for any loss, expense, or damage arising from the leakage of data stored in the machine or from the use of the machine.

Information assets in the machine

The machine may contain the following information assets:

1. Image data temporarily stored on the hard disk when copying or printing
2. Image data in copy and print jobs stored on the hard disk
3. User Tools data that includes confidential information, such as the address book, IP address, and mail server address
4. Registered Stamp and User Text data

For details, see the table.

Countermeasures

To protect your sensitive information, erase the data according to the methods listed in the table before disposing of or returning the machine.

Be sure to use Data Overwrite (Erase Memory) to erase the data on the hard disk and memory, since it is at risk of being recovered by special tools.

Properly deal with SD cards and USB flash drives containing your valuable information assets.

Even if you reformat your SD cards and USB flash drives, some of the data will remain undeleted.

When you dispose of or return the machine, use the Data Overwrite function to completely erase the data on all media.

For details about the Data Overwrite function, see the Security Reference.

* Depending on the model, your machine may not have the Data Overwrite function as a standard feature.

  If it does not, you will need to install the optional DataOverwriteSecurity Unit to erase data. If you do not have the DataOverwriteSecurity Unit but wish to erase data, contact your sales or service representative.

◆ Data that can be erased by the Data Overwrite function

Type of Data	How to Erase
• Image data temporarily stored on the hard disk under the copier, scanner, fax, and printer functions • Image data in stored files	The data on the hard disk is at the risk of being recovered by special tools that analyze the magnetic patterns on the disk. Before you dispose of or return the machine, erase the data using Data Overwrite.
• Captured images (image logs) • Registered data (Stamp, Programmed Format, and Form) • Registered fonts • Embedded Software Architecture applications' program data • Address Book • Specified settings in User Tools (such as the IP address)	Although this data can be erased using Web Image Monitor or the User Tools setting on the control panel, data remnants on the disk are at risk of being recovered by special tools that analyze the magnetic patterns on the disk. Erase the data using Data Overwrite.

For details, see the Security Reference.

◆ Data that cannot be erased by the Data Overwrite function

Type of Data	How to Erase
• User data stored in devices other than the hard disk, such as the user text, standard message, device certificate, site certificate, and SSH public key	Erase this data using Web Image Monitor or the User Tools setting on the control panel. For details about using Web Image Monitor, see the Web Image Monitor Help.
Data created by Embedded Software Architecture applications	Depending on the Embedded Software Architecture application, the data may be stored in the internal memory. If an Embedded Software Architecture application (GlobalScan NX or Card Authentication Package) is being used, contact your service representative.

Printed in Japan
EN (US) D572-7015
D5727015