KYOCERA MITA

Data Security Kit (B),

Overseas Security Target,

Version 0.15

This document is a translation of the security target written in Japanese, which has been evaluated and certified. The Japan Certification Body has reviewed and checked it.

October 21, 2005

KYOCERA MITA Corporation

- Revision History -

Date	Version	Content of revision	Approved	Drafter
Apr. 26, 2004	0.01	• Newly drafted	Yoshioka	Sone
Jun. 23, 2004	0.02	• Modifications of expressions and descriptions in general	Yoshioka	Sone
Aug. 6, 2004	0.03	• Modification of the items pointed-out in chapters one to three	Yoshioka	Sone
Sep. 14, 2004	0.04	• Modification of TOE identification • Modification of the items pointed-out in chapters one to eight	Yoshioka	Sone
Sep. 17, 2004	0.05	• Modification of TOE constitution • Modification of the version of TOE identification	Yoshioka	Sone
Oct. 21, 2004	0.06	• Support of ASE001-01, ASE002-01, ASE003-01, ASE004-01, and ASE005-01	Yoshioka	Sone
Nov. 17, 2004	0.07	• Support of ASE006-01, ASE007-01, ASE008-01, ASE009-01, ASE010-01	Yoshioka	Sone
Nov. 26, 2004	0.08	• Support of ASE011-01, ASE012-01, and ASE013-01	Yoshioka	Sone
Jan. 8, 2005	0.09	• Support of ASE014-01	Yoshioka	Sone
Jan. 19, 2005	0.10	• Changed the name of the Assurance requirements document	Yoshioka	Sone
Apr. 6, 2005	0.11	• Support of ASE015-01 • Changed the name of the assurance requirement document	Yoshioka	Sone
Apr. 26, 2005	0.12	• Changed "Person in charge of maintenance" to "Person in charge of service"	Yoshioka	Sone
Jun. 14, 2005	0.13	• Modified the descriptions related to O.METHOD • Modified the name for Table 6.2	Yoshioka	Sone
Aug. 4, 2005	0.14	• Partial modification of the descriptions of Table 6.2 • Partial modification of the documentations for assurance measures	Yoshioka	Sone
Oct. 21, 2005	0.15	• Added the descriptions related to OE.POWER	Yoshioka	Sone

- Table of contents -

- Table of contents of drawings –

- Table of contents of tables -

1. ST Introduction

1.1. ST Identification

1.1.1. ST Identification

Name:	KYOCERA MITA Data Security Kit (B) Overseas Security Target
Version:	Version 0.15
Creation Date:	October 21,2005
Producer:	KYOCERA MITA Corporation

1.1.2. TOE Identification

Name:	Data Security Kit (B) Software
Version:	V1.10E
Developper:	KYOCERA MITA Corporation

Note: Version 1.10E is constituted by the following ROM versions.

MAIN	: 29101B-0210.00
PRINTER	: 2FB_3F00.001.200

1.1.3. Used CC Version

ISO/IEC 15408:1999

Common Criteria CCIMB Interpretations(as of 15 February 2002)

Note: The Japanese versions are used as for the following materials.

- Common Criteria for Information Technology Security Evaluation Part 1: Overview and General Model, version 2.1, August 1999, CCIMB-99-031 (Japanese)
- Common Criteria for Information Technology Security Evaluation Part 2: Security Structure Requirements, version 2.1, August 1999, CCIMB-99-032 (Japanese)
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, version 2.1, August 1999, CCIMB-99-033 (Japanese)
- Common Criteria CCIMB Interpretations(as of 15 February 2002)

1.2. ST Overview

This ST describes the "Data Security Kit (B) Software" to be installed on the Multifunctional products (MFPs), the overseas versions of the "KM-8030 / KM-6030, CS-8030 / CS-6030," provided by KYOCERA MITA Corporation. MFPs are products that have printer functions and network scanner functions, besides the copying functions as a copier. (The copier, printer, and network scanner functions will be called ordinary functions, hereafter.) By using the MFPs, the users will be able to handle not only the outputted paper documents, but will also be able to treat them as electronized documents.

This TOE is a software module that is installed on the MFPs "KM-8030/KM-6030, CS-8030/CS-6030" as options, and which provides the ordinary functions, and also security functions for protecting residue data.

Security Functions to be provided by the TOE:

- A function to protect residue data after the processings of copying, printing, or network scanning, and also after logical deletions of data stored within the MFP.

1.3. CC Conformance

For security function requirements

Part 2 conformant

For security assurance requirements

Part 3 conformant

Evaluation assurance level

EAL 3 conformant

1.4. Reference Materials

- Common Criteria for Information Technology Security Evaluation
  Part 1: Introduction and general model
  August 1999 Version 2.1 CCIMB-99-031
- Common Criteria for Information Technology Security Evaluation
  Part 2: Security functional requirements
  August 1999 Version 2.1 CCIMB-99-032
- Common Criteria for Information Technology Security Evaluation
  Part 3: Security assurance requirements
  August 1999 Version 2.1 CCIMB-99-033
- Common Criteria CCIMB Interpretations(as of 15 February 2002)
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part1, 99/12
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part2, 99/12
- ISO/IEC 15408, Information Technology – Security techniques – Evaluation criteria for IT security – Part3, 99/12

2. TOE Description

2.1. TOE Type

This TOE is a software module product called "Data Security Kit (B) Software," and it provides security functions to the MFPs.

Note: Software modules providing ordinary functions are also included within the scope of the TOE.

2.2. Terminology

The definitions for the terms used in this ST are indicated in Table 2-1.

Table 2-1 Definitions of terms related to TOE

Terms	Definitions
Spool-storage	Keeping the received image data temporarily on the HDD, without outputting it or forwarding it as is. This is executed automatically during the process of the MFP, without the user being conscious about it. This should be compared to long period storage.
Long period storage	Keeping the received image data on the HDD for a long period. The users will have to consciously conduct the storage or reading operations for this storage. This should be compared to spool-storage.
Client PC	It indicates the computers that connect to the network, and utilize the TOE services (functions) of the TOEs that are connected to the network.
Network scanner	A function to transmit the scanned originals as image data, to the client PCs. There is PC transmission that transmits them via the LAN, e-mail transmission that transmits them via e-mails, and a TWAIN function that captures images of the originals by operations from the client PC.
PC transmission	This is a processing in which the scanned images are compressed into file formats specified by the user, and transmitted to the utilities of the specified client PC.
E-mail transmission	This is a processing in which the scanned images are compressed into file formats specified by the user, and transmitted to pre-registered e-mail servers, according to the SMTP protocol.
TWAIN	This is a processing in which the originals set on the MFP are captured into the client PCs by operations from the client PC, utilizing TWAIN compatible applications.

Job	A unit for one processing of the copier, printer, or network scanner functions. Image data of the originals are also included in this job.
Printing job	Jobs that are processed as printer functions, among the various jobs.
Management area	An area within the image data where management information for that data is recorded. A logical deletion of image data means making this area unrecognizable
Actual data area	An area within the image data where data composing the actual image is recorded. When an image data is logically deleted, this area will still remain. This remaining area will be called "residue data."
Printer driver	Software to be installed on the client PCs to control the printing functions of the MFP, such as transferring characters or images displayed on the client PC to the printer of the MFP.
e-MPS	It is an abbreviation for "enhanced Multiple Printing System." This is an expanded function of the printing function, and it is capable of executing various printing jobs based on data received from the client PC.
Data Security Kit (B) Hardware key	This is a circuit board whose installation is indispensable, when utilizing the security functions. It will be installed by the person in charge of service, when installing the Data Security Kit (B). If the hardware key for the Data Security Kit (B) is removed during operation, the security function will not become invalid, but the MFP itself will become unoperatable.
Operation panel	This is installed on the uppermost part of the MFP, and is constituted by a liquid crystal panel. It is an external interface, and users can utilize the TOE via this operation panel.
NIC	It is an abbreviation for "Network Interface Card." It is an expansion card for connecting the TOE to the internal network (LAN).
Scanner engine	It is a module for controlling the apparatus for scanning the originals.
Printing engine	It is a module for controlling the apparatus that outputs data onto the paper and prints.
Forms	This indicates the combining-source images that will become the source images for the function to superimpose images (combining of the images). Originals that have been read in can be superimposed and copied onto forms.

2.3. TOE Overview

2.3.1. The purpose of utilizing the TOE

This TOE will be installed on MFPs that are to be utilized in offices and schools, and will be utilized for the purpose of protecting image data remaining on the HDDs from unjust exposure, after various copying (duplication), printing (paper output), and network scanning (electronization) processings, by providing an HDD overwriting function.

2.3.2. The environment in which the MFPs are utilized

TOE installed MFPs will be used in offices and schools where various documents are handled, and they will be connected to the internal network (LAN). They can also be used by being connected to local ports (parallel port, USB port, serial port), for printer output.

The TOE machine administrators are able to conduct the operation/management of the MFPs via the LAN/local-port, by installing drivers and various utilities onto client PCs within the LAN, or onto locally connected client PCs. The TOE users can utilize the MFPs, via the LAN/local-port. However, when utilizing the MFP externally via the LAN/local port, it can only be utilized in inputting image data and outputting them through the MFP, and cannot be utilized to capture, via the LAN/local-port, image data stored on the MFP for a long period.

Fig. 2-1 indicates a common usage environment, in offices.

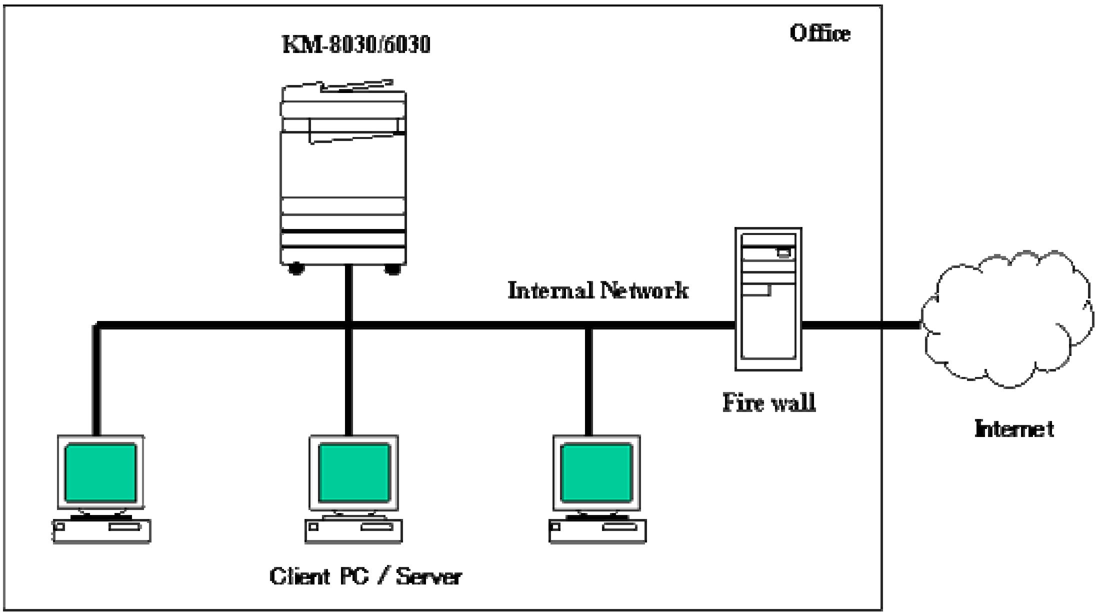

Fig. 2-1 A common usage in offices

2.3.3. People associated with the TOE

The TOE machine administrator, TOE user, and the person in charge of service for the TOE are defined as follows.

TOE machine administrator:

A person registered as the administrator of the main unit of the TOE installed MFP. The TOE machine administrator has privileges concerning the machine's main unit.

[Utilizing method]

The TOE machine administrator implements the installation and operation management of devices composing the TOE installed MFP. He/she also implements the operation management for maintaining the security of the TOE.

[Utilizing procedure]

- The TOE machine administrator conducts the setting and installation of each of the devices necessary for the operation of the TOE, according to the manuals of each of the devices and software.
- The TOE machine administrator registers/configures user information, if an individual setting of the users becomes necessary to let the TOE users utilize the MFPs.
- The TOE machine administrator installs software necessary for the operation and management of the MFP, to the client PCs, etc.
- The TOE machine administrator changes the setting for the overwriting method, executes the HDD formatting function, and changes the TOE administrator management code, using the TOE machine administrator interface.

TOE user:

People allowed to utilize TOE installed MFPs, in offices or schools. They are able to utilize the copying, printing, network scanning, and other functions. The attacking capability of the TOE users with respect to exposure of image data is at a low level.

[Utilizing method]

TOE users will copy, print, and network scan various documents.

[Utilizing procedure]

- TOE users will be using the copying, printing, and network scanning functions, according to the MFP and TOE manuals.

Person in charge of service:

A person approved by KYOCERA MITA as the person in charge of service for the TOE installed MFP. The person in charge of service will install the TOE, and conduct the maintenance of the TOE installed MFP.

[Utilizing method]

The person in charge of service should install the Data Security Kit (B) hardware key and start-up (enable) the TOE upon installing the TOE, and should also conduct the maintenance of the devices that constitute the TOE installed MFP, and the TOE. He/she also has a role as a TOE machine administrator, and in emergencies, can change the settings for the overwriting method, execute the HDD formatting function, and change the TOE administrator management code, with the approval of the TOE machine administrator, using the TOE machine administrator interface. (Details of each of the functions will be descibed later on)

[Utilizing procedure]

- The person in charge of service should install the Data Security Kit (B) hardware key, install the TOE, and start-up (enable) the TOE, according to the service manual of the MFP.
- The person in charge of service will conduct maintenances of devices constituting the TOE installed MFPs, and also the TOE, according to the service manual of the MFP.
- The person in charge of service changes the settings for the overwriting method, executes the HDD formatting function, and changes the TOE administrator management code, with the approval of the TOE machine administrator, using the TOE machine administrator interface.

2.4. TOE Configuration

2.4.1. Physical Configuration of the TOE

A conceptual diagram of the physical construction of TOE is indicated in Fig. 2-2.

The TOE refers to the software in the MAIN ROM and PRINTER ROM, which are on the main board and printer board, respectively.

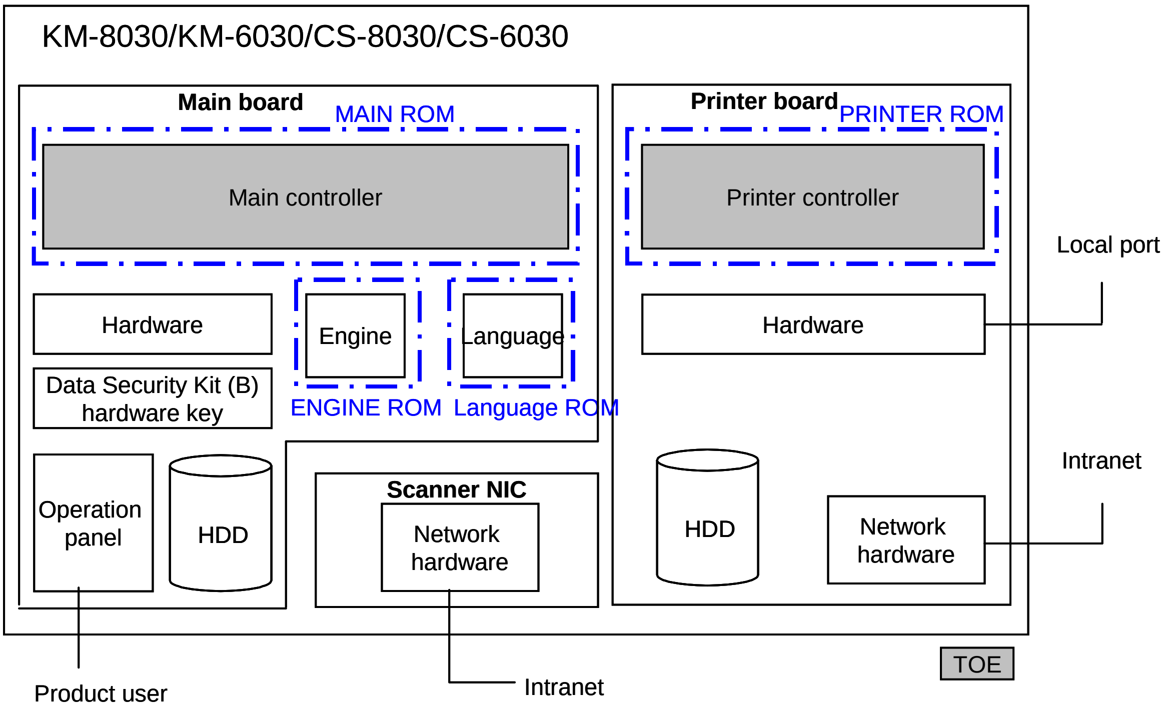

Fig. 2-2 Construction diagram of TOE

2.4.2. Operating environment of the TOE

The "KM-8030/KM-6030, CS-8030/CS-6030" are constituted by hardware and software.

The hardware part is comprised of the main board, network scanner NIC, and the printer board, and there are CPUs in each of the boards. There are also HDDs on each of the main and printer boards, and also network hardware for connecting to the network, on the network scanner NIC and printer board. There is a local port for connecting locally (parallel port, USB port, serial port), on the printer board.

The hardware key for the Data Security Kit (B) will be necessary to activate the TOE. If the Data Security Kit (B) hardware key is removed during operation, the security function will not become invalid, but the MFP itself will become unoperatable.

Other portions such as the CPU, memory, the scanner and printing portions are generically called "hardware," in Fig. 2-2.

There is a main controller within the MAIN ROM on the main board. The main controller is comprised of the copyier module, scanner module, network module, and a library common for both copying and network-scanning.

Besides these, there is also a language module and an engine module, as basic software for activating the TOE. They are stored in the language ROM and ENGINE ROM, respectively. If

necessary, the language ROM can be changed to cope with multiple languages. There are modules for controlling the scanner engine and printing engine, in the ENGINE ROM.
There is a printer controller within the PRINTER ROM on the printer board. The printer controller is comprised of the printer module, network module, printer library, and network service.

The specifications for the hardware, network hardware, and HDDs in Fig. 2-2 are indicated in Table 2-2.

Table 2-2 Specifications for the hardware, network hardware, and HDDs

Apparatus name	Type	Performance	Notes
Main board	CPU	Oscillation source : 8.29 MHz (Internal: 132 MHz)	-
	Memory	128 Mbyte	-
	HDD	20 Gbyte	-
Scanner NIC	Network hardware	10Base-T/100Base-Tx	-
Printer board	CPU	600 MHz	-
	Memory	64 Mbyte	Optional RAM 32 to 256 MByte
	HDD	10 Gbyte	-
	Network hardware	10Base-T/100Base-Tx	-

2.4.3. Software that constitute the TOE

Software constituting the TOE are indicated in Table 2-3. The shaded portions indicate the TOE.

Table 2-3 Software that constitute the TOE

Name of ROM	Type		Notes
MAIN ROM	Main controller		-
		Copier module	-
		Scanner module	-
		Network module	-
		Library common for both the copier and	The HDD Overwrite

		network scanner	Function and the administrator authenticating function are included in it
ENGINE ROM	Engine module		Scanner engine Printer engine
Language ROM	Language module		Character string data It is set to the destination region
PRINTER ROM	Printer controller		-
		Printer module	-
		Network module	-
		Library for the printer	The HDD Overwrite Function is included in it
		Network service	-

2.4.4. Logical Configuration of the TOE

A conceptual diagram of the logical construction of the TOE is indicated in Fig. 2-3.

The TOE has not only security functions, but also ordinary MFP functions such as copying functions. The following functions are included within the logical scope of TOE.

- HDD Overwrite Function

  A function that completely erases the actual data area by overwriting meaningless character strings onto them, after data stored in the HDD have been logically deleted.
- Administrator authenticating function

  A function to identify and authenticate a TOE machine administrator, with the TOE administrator management code inputted from the operation panel.
- Copier function

  A function to read image data from the scanner of the MFP, and output them from the printing portion of the MFP.
- Network scanner function

  A function to read image data from the scanner of the MFP, and transmit them to client PCs.

  There is PC transmission that transmits them via the LAN, and e-mail transmission that sends them with e-mails.

  There is also TWAIN, in which the originals set on the MFP are captured into the client

PC by operations from the client PC, by utilizing applications that support TWAIN.

- Printer function

  A function to output image data transmitted from client PCs on the LAN, or from a locally connected client PC, from the printing part of the MFP.

- Job management function

  A function to administer jobs/printing-jobs stored on the HDD. The jobs/printing-jobs can be edited, outputted, or deleted.

The following function is logically constituted as a function outside the TOE.

- User interface function

  A function to accept inputs/operations from the operation panel. It also makes displays on the operation panel.

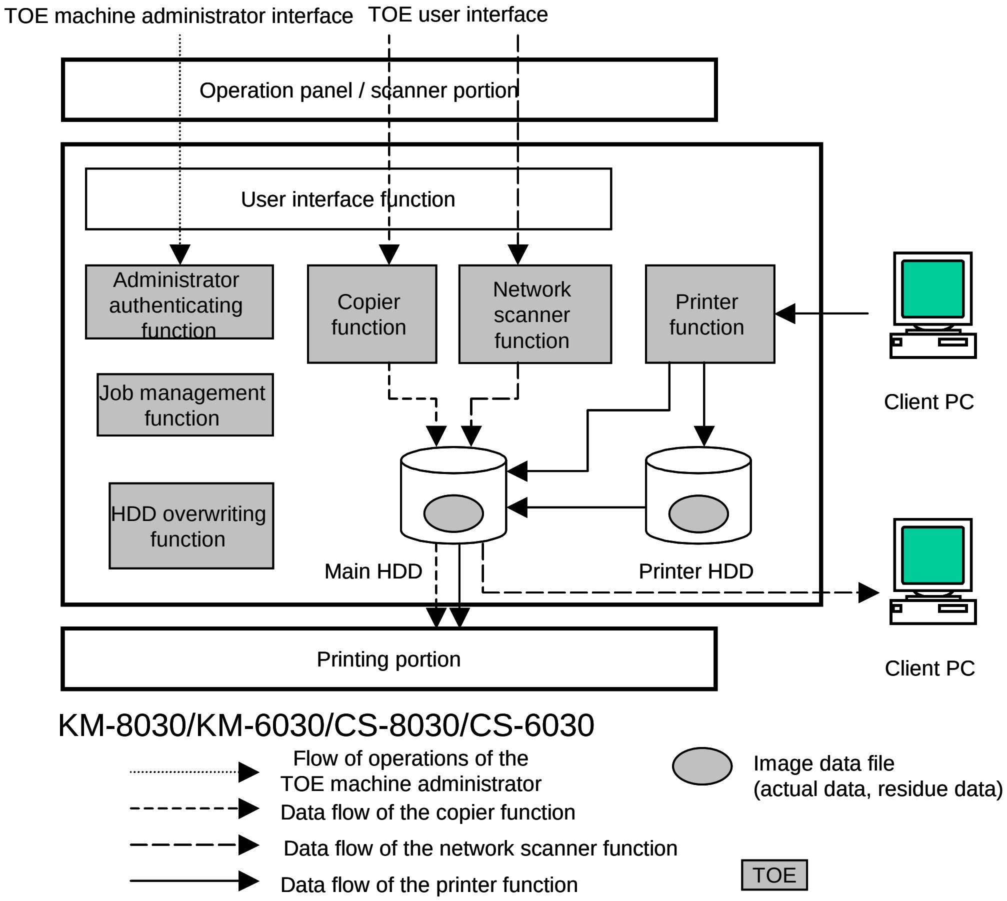
TOE machine administrator interface
TOE user interface
Operation panel / scanner portion
User interface function
Administrator authenticating function
Copier function
Network scanner function
Printer function
Client PC
Job management function
HDD overwriting function
Main HDD
Printer HDD
Client PC
Printing portion
KM-8030/KM-6030/CS-8030/CS-6030
Flow of operations of the TOE machine administrator
Data flow of the copier function
Data flow of the network scanner function
Data flow of the printer function
Image data file (actual data, residue data)
TOE

Fig. 2-3 Logic diagram of the TOE

2.5. TOE functions

The Functions to be provided by TOE are the following.

- Security Functions
  - HDD Overwrite Function
  - Administrator authenticating function
- Ordinary functions as an MFP
  - Copier function
  - Network scanner function
  - Printer function
  - Job management function

2.5.1. TOE Security Functions

2.5.1.1 HDD Overwrite Function

There is an HDD overwriting function in addition to the conventional logical delete processing, with a purpose of improving safety furthermore.

When using the copier function, network scanner function, or the printer function, and then deleting the image data stored in the HDD, meaningless character strings are overwritten onto the actual data area after those image data are logically deleted, to completely erase the actual data area.

There is a 3-time Overwrite method and a Once Overwrite method, for the overwriting method.

◆ 3-time Overwrite

Random data (1), random data (2), and NULL (0x00) are written in sequence, to all the actual data area of the data to be overwritten.

◆ Once Overwrite

NULL (0x00) is written to all the actual data area of the data to be overwritten.

2.5.1.2 Administrator authenticating function

It identifies and authenticates a TOE machine administrator, with the TOE administrator management code inputted from the operation panel.

An identified and authenticated TOE machine administrator can execute an "HDD formatting function" that overwrites the whole area of the HDD, and can change the HDD overwriting function between the 3-time Overwrite method and Once Overwrite method.

The 3-time Overwrite method is the initial default, and it should be set when more importance is to be attached to safety than processing efficiency. The 1-time Overwrite method should be set when more importance is to be attached to efficiency. Either of the methods will always be set, and the default setting is the 3-time Overwrite method.

2.5.2. Ordinary functions

The TOE provides the following basic functions. Upon using these functions, and when image data kept on the HDD are processed with the conventional logical deletion, the "HDD overwriting function," which is a secutrity function, will function.

■ Copier function

The copying of the originals read in from the scanner is conducted by the TOE users. (Ordinary copying)

When this ordinary copying is executed, the image data is spool-stored onto the HDD of the main board, and will be deleted when the output has been completed.

This copier function also includes a document management function.

There is a Shared Data Box, Synergy Print Box, and a Form Box for the document management function. Each of the boxes exists onto the HDD of the main board.

[**Document Management Functions**]

- Shared Data Box –

  Image data of the originals read in from the scanner can be stored in the boxes as jobs, and the stored jobs can be outputted when necessary.

- Synergy Print Box –

  The originals read in from the scanner, or image data transmitted from the printer driver can be stored in the boxes as jobs. They are stored by specifying the number of the Synergy Print Box. The stored jobs can be outputted when necessary. The stored jobs can be consolidated when outputting them. It is also possible to set a storage period of one to seven days for the boxes, and the boxes will be deleted when the specified storage period from the stored date elapses.

- Form Box –

  It is possible to pre-register forms to be combined upon copying.

  The originals read in from the scanner, or image data transmitted from the printer driver can be registered in the boxes as forms.

■ Network scanner function

TOE users can transmit the image data of originals read in from the scanner, to the client PCs. There is PC transmission that transmits them via the LAN, and e-mail transmission that sends them via e-mails.

The originals set on the MFP can be captured into a client PC by operations from the client PC, utilizing applications that support TWAIN.

When using the network scanner function, the image data is spool-stored onto the HDD of the main board, and will be deleted when the transmission has been completed.

Caution: It is not possible to capture images through PC transmission, e-mail transmission, or TWAIN, using jobs stored with the document management function.

■ Printer function

Image data transmitted from the printer driver are outputted to the papers, by the TOE users (ordinary printing). There are outputs via the LAN, and outputs via the local port.

The printer function also has the following expanded functions (e-MPS), besides the function to simply output data.

When using the printer function, the image data is temporarily spool-stored onto the HDD of the main board, and will be deleted when the output has been completed, in both the ordinary printing and expanded printing functions.

[Expanded functions (e-MPS)]

- Temporary code Job –

  It stores printing jobs onto the HDD of the printer board, temporarily. The older ones will be deleted when it exceeds the capacity of the temporary storage area. The stored printing jobs can be outputted when necessary.
- Permanent code Job –

  Permanently stores printing jobs onto the HDD of the printer board. They will not be deleted until a TOE user deletes them. The stored printing jobs can be outputted when necessary.
- Synergy Print Box –

  It stores printing jobs into the Synergy Print Box on the main board. They are transmitted by specifying the number of the Synergy Print Box.
- Form Gallery –

  It stores printing jobs into the Form Box on the main board.
- Quick Copy –

  It temporarily stores printing jobs onto the HDD of the printer board after outputting them, so that they can be outputted again. The stored printing jobs are deleted when the power is turned off. (Actually, the delete processing is executed when the power is turned on the next time) The older ones will be deleted when it exceeds the capacity of the storage area.
- Proof and Hold –

A portion of the printing job is outputted and then the job is stored onto the HDD of the printer board, so that they can be outputted after confirming its content. The stored printing jobs are deleted when the power is turned off. (Actually, the delete processing is executed when the power is turned on the next time) The older ones will be deleted when it exceeds the capacity of the storage area.

- Virtual MailBox (VMB) –

  It stores printing jobs into the virtual mailbox installed on the HDD of the printer board. The stored printing jobs are not printed at the time they are transmitted, but outputted when the mail box number is specified from the operation panel of the main unit of the machine. The printing jobs will be deleted when they have been outputted.

- Private Print –

  Access codes are added to the printing jobs, and stored temporarily onto the HDD of the printer board. The stored printing jobs are not printed at the time they are transmitted, but are outputted when the corresponding access code is inputted from the operation panel of the main unit of the machine. The printing jobs will be deleted when they have been outputted. The stored printing jobs are deleted when the power is turned off. (Actually, the delete processing is conducted when the power is turned on the next time)

- Stored Job –

  It is a function equivalent to private printing, but the stored printing job will not be deleted even when the power is turned off.

■ Job management function

It is a function included in the copier and printer functions.

The jobs/printing-jobs stored on the HDD are administered by each of the functions. It is possible to edit, output, or delete the jobs/printing-jobs.

It can be operated from the operation panel, or from utilities (described below) in the client PC.

[About the utilities]

Above-mentioned function can be supported by installing various tools onto the client PC.

- "KM-NET Printer Disk Manager," "KM-NET for Clients" -

  Job management function operations will be executed to edit, output, or delete the printing jobs stored on the HDD of the printer board.

  "KM-NET Printer Disk Manager" is a tool for the TOE machine administrators, and "KM-NET for Clients" is a tool for the TOE users.

- Printer driver -

This will become necessary when using the printer function.

All of the settings necessary when expanded functions are used, will also be conducted from the printer driver.

- Scanner File Utility –

  It will become necessary when executing PC transmission for the the network scanner function.

  Image data transmitted from the TOE is received, and the data is stored in the specfied folder. (It can be folders in the PC itself, or shared folders via the network)

- Twain driver -

  It will become necessary when conducting TWAIN of the network scanner function.

  It is called up from commercially available image processing applications, and reads the originals set on the TOE and captures the image data, by operations from the TWAIN driver.

If there are any instructions of the copying/printing/network-scanning functions given simultaneously, or in overlap, they will be processed sequentially according to the priority order, for all the ordinary functions. Therefore, all the processings will always be completed to the last one, even if they are not processed immediately after their instructions are given.

It is also possible to stop the copier/printing/network-scanner function processings before they are completed, by instructions from the TOE users.

Table 2-4 indicates a list of relationships between the TOE functions, the places of storage of image data, and the deleting means.

Table 2-4 The TOE functions, places of storage, and the deleting means

Basic functions	Detailed functions	Places of storage	Storage mode	Deleting means
Copier function	Ordinary copying	Main HDD	Spool-storage	After the processing has been completed, or cancelled
	Shared Data Box	Main HDD	Long period storage	After there has been deleting operations from the operation panel, or cancellations of document registrations
	Synergy Print Box	Main HDD	Long period storage	After there has been deleting operations from the operation panel, automatic deletion after a "one to seven day storage period" has elapsed, or cancellations of document registrations
	Form Box	Main HDD	Long period storage	After there has been deleting operations from the operation panel, or cancellations of document registrations
Network scanner function	PC transmission / E-mail transmission / TWAIN	Main HDD	Spool-storage	After the processing has been completed, or cancelled

Printer function	Ordinary printing	Main HDD	Spool-storage	After the processing has been completed, or cancelled
	Temporary code Job	Printer HDD	Long period storage	After there have been deleting operations from the utilities, or after the oldest job is deleted upon trying to store exceeding the storage area, or after cancelling job registration processings
	Permanent code Job	Printer HDD	Long period storage	After there have been deleting operations from the utilities, or cancellations of job registrations
	Synergy Print Box	Main HDD (Synergy Print Box)	Long period storage	After there have been deleting operations from the operation panel, automatic deletion after a "one to seven day storage period" has elapsed, or cancellations of job registrations
	Form Gallery	Main HDD (Form Box)	Long period storage	After there have been deleting operations from the operation panel, or cancellations of job registrations
	Quick Copy	Printer HDD	Long period storage	After there have been deleting operations from the operation panel, or after it is deleted upon power-on after the power has been turned off, or after the oldest job is deleted upon trying to store exceeding the storage area, or after cancelling job registration processings
	Proof and Hold	Printer HDD	Long period storage	After there have been deletions from the operation panel, or after it is deleted upon power-on after the power has been turned off, or after the oldest job is deleted upon trying to store exceeding the storage area, or after cancelling job registration processings
	Virtual MailBox	Printer HDD	Long period storage	After there have been deleting operations from the operation panel or utilities, or after an output has been completed, or after cancelling job registrations
	Private Print	Printer HDD	Long period storage	After there have been deleting operations from the operation panel, or after an output has been completed, or after it is deleted upon power-on after the power has been turned off, or after cancelling job registrations
	Stored Job	Printer HDD	Long period storage	After there have been deleting operations from the operation panel, or cancellations of job registrations

2.6. Assets to be protected

When conducting copying/printing/network-scanning processings, MFPs in general conduct the processings after storing the data temporarily in a spool-storage area, and only logically delete the management area of those data after the processing has finished. For this reason, the actual data area will remain as "residual information." Since the same type of data as those processed in the copying/printing/network-scanning processings is in this residual information, it may happen that these data are wholly taken out, if they were to be accessed in any way. In some cases, there may be confidential information of the users included in these data, and it may pose serious problems if they were taken out.

Such being the case, the assets that should be protected by TOE will be indicated in the following.

■ Residue data

Residue data of the image data spool-stored or stored for a long period in the HDD of the main board, and which has been logically deleted; and
Residue data of the image data stored for a long period within the HDD of the printer board, and which has been logically deleted

Data subject to this are stored in the following files.
(The following are the types of image data to be stored in the HDD)

◆ Image data files on the HDD of the main board

- Spool-stored jobs during ordinary copying
- Jobs within the Shared Data Box
- Jobs within the Synergy Print Box
- Jobs within the Form Box
- Spool-stored jobs during network scanning (PC transmission / e-mail transmission / TWAIN)
- Spool-stored jobs when the ordinary printing functions of the printer were used, or when any of the printer expansion functions were used

◆ Image data files on the HDD of the printer board

- Printing jobs of the printer expansion function "temporary storage"
- Printing jobs of the printer expansion function "permanent storage"
- Printing jobs of the printer expansion function "quick copy"
- Printing jobs of the printer expansion function "Proof and Hold"
- Printing jobs of the printer expansion function "virtual mailbox"
- Printing jobs of the printer expansion function "private print"
- Printing jobs of the printer expansion function "Stored Job"

3. TOE Security Environment

3.1. Assumptions

The following assumptions are necessary for an operating environment to let the TOE be allocated at a safe operating environment.

A.PHYSICAL: Physical safety of the TOE and assets

MFPs with TOE installed should be installed at physically protected places, where only people associated with the TOE are able to use it.

A.ADMIN: reliability of the administrators

The TOE machine administrator should be a reliable person, and someone who will not do anything dishonest.

A.CE: reliability of the person in charge of service

The person in charge of service of the TOE should not do anything dishonest.

3.2. Threats

We will describe the threats that can be assumed under the operating environment indicated in the assumption.

The level of the attacking capability of the attackers assumed for this TOE is at a low level.

T.AGAIN: illegal accessing of residue data

Malicious TOE users connecting illegal decoding apparatuses to the HDDs, or taking out the HDDs, to browse/output the residue data kept on the HDDs. Or to browse/output the residue data on HDDs that have not been overwritten completely because the power of the MFP has gone off during overwriting.

3.3. Organizational Security Policies

The TOE needs to observe the following, as an organization security policy.

P.METHOD: Application of the overwriting method

The 3-time Overwrite method or the Once Overwrite method should be applied when overwriting an HDD, taking into consideration the balance between safety and efficiency.

4. Security Objectives

4.1. Security Objectives of the TOE

We will be describing the security objectives to be implemented by TOE to counter the threats.

O.REMAIN: Overwriting of residue data

The TOE has to overwrite the storage area of residue data, so that residue data stored on the HDDs will not be illegally browsed/outputted.

O.METHOD: a function to set the overwriting method

The TOE must provide a function to set the HDD overwriting function to either the 3-time Overwrite method or the Once Overwrite method, to the TOE machine administrators.

4.2. Security Objectives for the Environment

We will be describing the security objectives to be implemented by the TOE environment, to counter the threats, or to realize the assumptions.

OE.PHYSICAL: Physical protection of the TOE and assets

The TOE machine administrator should install the TOE installed MFPs at places where room entrance/exit management is being executed, and places where only people associated with the TOE are able to use, so that suspicious characters will not be able to use the TOE freely.

OE.ADMIN: Selection of the administrator

The organization installing the TOE should select an appropriate person who will execute his/her assigned role faithfully, and not do anything dishonest, for the TOE machine administrator.

OE.CE: Monitoring of the person in charge of service

When the person in charge of service conducts maintenance, etc., the TOE machine administrator should always monitor it.

OE.POWER: Prevention of power off

If the power goes off while using MFPs with TOE installed, TOE users should promptly turn on the power again.

5. IT Security Requirements

5.1. TOE Security Requirements

5.1.1. TOE Security Functional Requirements

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1

The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.

[assignment: *list of feedback*]

- Dummy characters (*)

  Note: Dummy characters with the same length as the number of characters inputted

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]

- Numbers (0 to 9): eight figures, fixed

[Details: secrets]

- TOE administrator management code

Dependencies: No dependencies

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to*, *deallocation of the resource from*] the following objects: [assignment: *list of objects*].

[selection: *allocation of the resource to, deallocation of the resource from*]

- *deallocation of the resource from*

[assignment: *list of objects*]

- Image data files on the HDD of the main board
- Image data files on the HDD of the printer board

Dependencies: No dependencies

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [selection: *change default, query, modify, delete, clear,* [assignment:*other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].

[assignment: *list of TSF data*]

- TOE administrator management code

[selection: *change default, query, modify, delete, clear,* [assignment:*other operations*]]

- query, modify

[assignment:*other operations*]

- none

[assignment: *the authorized identified roles*]

- TOE machine administrator

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

[assignment: *list of functions*]

- HDD Overwriting Function

[selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

- *modify the behaviour of, enable*

[assignment: *the authorised identified roles*]

- TOE machine administrator

Dependence: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [assignment: *the authorized identified roles*].

[assignment: *the authorized identified roles*]

- TOE machine administrator

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [assignment: *list of security management functions to be provided by the TSF*].

[assignment: *list of security management functions to be provided by the TSF*]

- Shown in Table 5-1. Control Item List.

Table 5-1 Control Item List

Function Requirement	Control Requirement	Control Item
FIA_UAU.2	Management of the authentication data by an administrator	Management of the TOE administrator management code, by the administrator
FIA_UAU.7	There are no management activities foreseen.	None
FIA_UID.2	The management of the user identities.	None (the TOE machine administrators are the only targets of identification, and since the TOE identifies the TOE machine administrators by having them conduct an operation designated for administrators, there is no need to administer user-identities)
FIA_SOS.1	the management of the metric used to verify the secrets.	None (the metric for secrets is a number with a fixed length of 8 figures, and there is no need to administer them)
FDP_RIP.1	The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE.	None (there is no need to administer the timing for the residual information protection, because it is implemented only when the assignments are released)

Function Requirement	Control Requirement	Control Item
FMT_MTD.1	managing the group of roles that can interact with the TSF data.	None (because the only roles are as TOE machine administrators, and management actions are not necessary)
FMT_MOF.1	managing the group of roles that can interact with the functions in the TSF.	None (because the only roles are as TOE machine administrators, and management actions are not necessary)
FMT_SMR.1	managing the group of users that are part of a role.	None (because there are no groups for users, and the only users to be associated to roles are the "TOE machine administrators," and management actions are not necessary)
FMT_SMF.1	There are no management activities foreseen.	None
FPT_RVM.1	There are no management activities foreseen.	None

Dependencies: No dependencies

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

5.1.2. TOE Security Assurance Requirements

The assurance level of the TOE security assurance requirements is EAL3. A list of the selected TOE security assurance requirements can be identified in Table 5-2. There are no specific assurance measures that will exceed EAL3.

Table 5-2 TOE Security Assurance Requirements

Security Class	Assurance Components	
Configuration management	ACM_CAP.3	Authorisation controles
	ACM_SCP.1	TOE CM coverage
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.2. Security Requirements for the IT Environment

There is no security requirement due to the IT environment, with which the TOE must comply.

5.3. Minimum Strength of Function

The "minimum strength of function" claim for the security function requirements is SOF-basic for this whole TOE.

The function requirements in which the "security strength of function" is required are the following, and the specified "strength of function" for each of them is also indicated in the following.

- FIA_UAU.2 - Strength of function: SOF-basic
- FIA_UAU.7 - Strength of function: SOF-basic
- FIA_SOS.1 - Strength of function: SOF-basic

6. TOE Summary Specifications

6.1. TOE Security Functions

Security Functions that should be provided by this TOE will be defined here.

Table 6-1 indicates the relationship between each of the TOE summary specifications and the security function requirements.

Table 6-1 TOE Summary Specifications and Security Function Requirements

Summary Specifications / Function Requirements	SPF.AGAIN	SPF.ADMIN
FIA_UAU.2		X
FIA_UAU.7		X
FIA_UID.2		X
FIA_SOS.1		X
FDP_RIP.1	X	
FMT_MTD.1		X
FMT_MOF.1		X
FMT_SMR.1		X
FMT_SMF.1		X
FPT_RVM.1	X	X

6.1.1. HDD Overwrite Funciton

The HDD overwriting function provides the following functions.

SPF.AGAIN

The HDD overwriting function is a function that overwrites all the actual data area of data stored on the HDD, not only deleting the management information of that data logically.

There are the following two methods for overwriting, and only TOE machine administrators can change it.

The default setting is the 3-time Overwrite method.

- 3-time Overwrite

Random data (1), random data (2), and then NULL (0x00) data will be written in sequence, to all the actual data area of the data to be overwritten.

- Once Overwrite

  NULL (0x00) data is written to all the actual data area of the data to be overwritten.

The HDD overwriting function is executed independently for each of the HDDs of the main and printer boards.

However, the setting of either of the overwriting methods, and the execution of the HDD formatting function, which is described below, will be conducted in unification for the HDDs of the main and printer boards, without distinguishing between them.

The HDD overwriting function can be executed in either of the following timings.

- When a job is deleted by an output, power off, or a deleting operation
- When an HDD formatting function is executed by the TOE machine administrator

  Note: In overwriting upon power off, the erase-processing is actually conducted when the power is turned on the next time.

This HDD overwriting function is always called out in above-mentioned timings, and executed without taking bypasses.

Overwriting function for the HDD on the main board

The overwriting function for each of the jobs stored in the image data files of the HDD on the main board is like the following.

■ A function to completely erase the data spool-stored on the HDD

Data to be spool-stored on the HDD are the following.

- Spool-stored jobs upon copying
- Spool-stored jobs during network scanning (PC transmission / e-mail transmission / TWAIN)
- Spool-stored jobs when ordinary printing functions, or any of the printer expansion functions of the printer were used

The timing at which data spool-stored on the HDD are overwritten has the following patterns.

- After finishing the processings of copying, printing (including the ordinary printing functions, and all of the printing expansion functions), and network-scanning, normally
- After these processings have been cancelled by a cancellation operation

- A function to completely erase the data stored on the HDD for a long period, by deleting operations of TOE users.

  The deleting operation can be executed from the operation panel.

  When a storage period is specified for the Synergy Print Box, data will be deleted not only by the deleting operations of TOE users, but also when the specified period has elapsed.

  Data to be stored on the HDD for a long period are the following.

  - Jobs within the Shared Data Box
  - Jobs within the Synergy Print Box
  - Jobs within the Form Box

  Overwriting will also be executed when a processing has been cancelled by a cancellation operation, during the storage of above-mentioned data onto the HDD.

Overwriting function for the HDD on the printer board

The overwriting function for each of the jobs stored in the image data files of the HDD on the printer board is like the following.

- A function to completely erase the data stored on the HDD for a long period, by deleting operations of TOE users.

  The deleting operation can be executed from the operation panel, and from related utilities.

  Data to be stored on the HDD for a long period are the following.

  - Printing jobs of the printer expansion function "Temporary code Job"
  - Printing jobs of the printer expansion function "Permanent code Job"
  - Printing jobs of the printer expansion function "quick copy"
  - Printing jobs of the printer expansion function "Proof and Hold"
  - Printing jobs of the printer expansion function "virtual mailbox"
  - Printing jobs of the printer expansion function "private print"
  - Printing jobs of the printer expansion function "Stored Job"

  Overwriting will also be executed when a processing has been cancelled by a cancellation operation, during the storage of above-mentioned data onto the HDD.

- A function in which data stored on the HDD for a long period is completely erased by an output

Data to be stored on the HDD for a long period are the following.

- Printing jobs of the printer expansion function "virtual mailbox"
- Printing jobs of the printer expansion function "private print"

■ A function in which data stored on the HDD for a long period is completely erased by a power off

Data to be stored on the HDD for a long period are the following.

- Printing jobs of the printer expansion function "quick copy"
- Printing jobs of the printer expansion function "Proof and Hold"
- Printing jobs of the printer expansion function "private print"

HDD formatting function

A function to completely erase data stored on the HDDs of the main and printer boards, when the TOE machine administrator executes this function.

■ It overwrites all the areas of the HDDs on the main and printer boards.

The overwrite processing will be executed in parallel timing for each of the HDDs.

[Note]

When power is cut off during overwriting, the residue data being overwritten will still remain on the HDD, but the overwrite processing will resume upon the next power on, and the residue data will be completely overwritten, in any of the "overwriting of the HDD on the main board," "overwriting of the HDD on the printer board," and "HDD formatting" functions.

6.1.2. Administrator authenticating function

An administrator authenticating function provides the following functions.

SPF.ADMIN

The administrator authenticating function is a function to securely identify and authenticate TOE machine administrators.

When a function that requires TOE machine administrator authority is accessed, the accessing person is identified whether he/she is a TOE machine administrator, and then the TOE administrator management code is required to be inputted, and the accessing person is to input the TOE administrator management code from the operation panel. Access will be granted if the inputted TOE administrator management code matches, but will not be granted unless it matches. Dummy characters (*) with the same length as the inputted characters will be displayed on the operation panel, during the authentication.

The metric for the TOE administrator management code is constituted by numbers (0 to 9), with a fixed length of 8 figures.
This administrator authenticating function is always called out when a function that requires TOE machine administrator authority is accessed, and executed without taking bypasses.

The TOE administrator management code setting is stored at a certain place, and although there is a default setting for when a machine is to be installed, it is made so that it can only be changed by the TOE machine administrator. When changing the TOE administrator management code, inputs other than numbers will not be accepted, and it will not be changed if it is shorter than 8 figures long.

The authorities given to a TOE machine administrator are the following.

- Changing the setting for the overwriting method (3-time Overwrite method / Once Overwrite method)
- Executing the HDD formatting function
- Changing the TOE administrator management code

6.2. Security Mechanisms

The TOE adopts the following security mechanisms.

■ 3-time Overwrite

A 3-time Overwrite method is one of the erasing algorithms for data on non-volatile memories.
It is an algorithm that writes random data (1), random data (2), and NULL (0x00) data in sequence, to all the actual data area of the data to be overwritten.

In this TOE, this method is used for the following function.

- HDD Overwrite Function

  When deleting data stored on the HDD, its actual data area is securely overwritten with the 3-time Overwrite method.
  Data is overwritten more safely than the Once Overwrite method.

■ Once Overwrite

A 1-time Overwrite method is one of the erasing algorithms for data on non-volatile memories.
It is an algorithm in which NULL (0x00) data is written to all the actual data area of the data

to be overwritten.

In this TOE, this method is used for the following function.

- HDD Overwrite Function
  When deleting data stored on the HDD, its actual data area is securely overwritten with the 1-time Overwrite method.

■ TOE administrator management code

The administrator authenticating function with the TOE administrator management code uses an authenticating mechanism.
It is constituted by numbers (0 to 9), with a fixed length of 8 figures.

In this TOE, this method is used for the following function.

- Administrator authenticating function
  It identifies and authenticates with the TOE administrator management code, when a function that requires TOE machine administrator authority is accessed.

6.3. Security Strength of Function

The security function of this TOE, which is based on a probabilistic or permutational mechanism, is an administrator authenticating function (SPF.ADMIN) corresponding to FIA_UAU.2, FIA_UAU.7, FIA_SOS.1, and the "security strength of function" of this function is SOF-basic.

6.4. Assurance Measures

A developer should conduct his/her developments according to the CC assurance requirements, and in-company development rules. The components of the EAL3 security assurance requirements, and the asurance documents that satisfy each of the assurance requirements are indicated in Table 6-2.

Table 6-2 Assurance Measures

Security Assurance Requirements		Assurance Measures
Configuration management	ACM_CAP.3	• KM-8030/KM-6030 Planning sheet for configuration management

		• KM-8030/KM-6030 Rule sheet for configuration management • KM-8030/KM-6030 Configuration list for the overseas versions
	ACM_SCP.1	• KM-8030/KM-6030 Planning sheet for configuration management • KM-8030/KM-6030 Rule sheet for configuration management
Delivery and operation	ADO_DEL.1	• KM-8030/KM-6030 Delivery procedure manual
	ADO_IGS.1	• Data Security Kit (B) Operation Guide • INSTALLATION GUIDE for Data Security Kit (B) • Printing System (V) Operation Guide Set-up Edition • Scan System (G) Operation Guide Set-up Edition • 8030/6030 SERVICE MANUAL
Development	ADV_FSP.1	• KM-8030/KM-6030 Function specification sheet
	ADV_HLD.2	• KM-8030/KM-6030 High-level designing sheet
	ADV_RCR.1	• KM-8030/KM-6030 Function support list
Guidance documents	AGD_ADM.1	• Data Security Kit (B) Operation Guide
	AGD_USR.1	• Data Security Kit (B) Operation Guide • 6030/8030 Operation Guide • 6030/8030 Advanced Operation Guide • Printing System (V) Operation Guide Function Edition • Printing System (V) Operation Guide Set-up Edition • Scan System Operation Guide Function Edition • Scan System (G) Operation Guide Set-up Edition
Life cycle support	ALC_DVS.1	• KM-8030/KM-6030 Regulation sheet for development security
Tests	ATE_COV.2	• KM-8030/KM-6030 Analysis sheet for the coverage test
	ATE_DPT.1	• KM-8030/KM-6030 High-level designing test specification
	ATE_FUN.1	• KM-8030/KM-6030 Functional test specification

		sheet
	ATE_IND.2	• TOE
Vulnerability assessment	AVA_MSU.1	• Data Security Kit (B) Operation Guide • 6030/8030 Operation Guide • 6030/8030 Advanced Operation Guide • Printing System (V) Operation Guide Function Edition • Printing System (V) Operation Guide Set-up Edition • Scan System Operation Guide Function Edition • Scan System (G) Operation Guide Set-up Edition
	AVA_SOF.1	• KM-8030/KM-6030 Analysis sheet of vulnerability
	AVA_VLA.1	• KM-8030/KM-6030 Analysis sheet of vulnerability

7. PP Claims

There is no conformance to a PP in this ST.

8. Rationale

8.1. Security Objectives Rationale

8.1.1. Compatibility of Security Objectives for Threats and Organization Security Policies

The relationship of the security objectives corresponding to threats and organization security policies is indicated in "Table 8-1 The correspondence of threats and organization security policies, to the security objectives".

Table 8-1 The correspondence of threats and organization security policies, to the security objectives

Threats/ Organization Security Policies Security Objectives	T.AGAIN	P.METHOD
O.REMAIN	X	
O.METHOD		X
OE.POWER	X	

The rationale for "Table 8-1 The correspondence of threats and organization security policies, to the security objectives" is indicated in the following.

T.AGAIN

In order to counter the threats of T.AGAIN, it has to be made so that it will not be possible to access the residue data kept on the HDD, after it is stored.

It is possible to counter this threat with the policies of O.REMAIN **and OE.POWER**. In other words, it is possible to prevent the residue data from being browsed/outputted, by overwriting the storage area of the residue data kept on the HDD, with O.REMAIN.

When the power of MFP is turned off during overwriting, the overwriting process is suspended, which may allow residue data, which has not been completely overwritten, to remain on the HDDs. To counter this threat, the TOE users should promptly turn on the power again in the case of the power going off while using MFPs by OE.POWER. By turning on the power, overwriting is re-executed automatically, so that it is possible to prevent unauthorized browsing/output of the residue data.

P.METHOD

Owing to the organization security policy P.METHOD, the administrator has to apply either the 3-time Overwrite method or the Once Overwrite method as the overwriting method, taking into consideration the balance between safety and processing efficiency. The P.METHOD can be realized, because a function to set the HDD overwriting function to either the 3-time Overwrite method or the Once Overwrite method is provided to the TOE machine administrators as a countermeasure policy of O.METHOD, as a countermeasure for the above.

8.1.2. Compatibility of the "security objectives for the environment" to the assumptions

The "security objectives for the environment" that support the assumptions are indicated in "Table 8-2 Assumptions and Security Objectives for the Environment Support".

Table 8-2 Assumptions and Security Objectives for the Environment Support

Assumptions Security Objectives for the Environment	A.PHYSICA	A.ADMIN	A.CE
OE.PHYSICAL	X		
OE.ADMIN		X	
OE.CE			X

The rationales for "Table 8-2 Assumptions and Security Objectives for the Environment Support" are indicated in the following.

A.PHYSICAL

A.PHYSICAL requires that TOE installed MFPs be installed at physically protected places, where only people associated with the TOE are able to use it. This is for the purpose of not letting an unspecified large number of people from using the TOE, in order to limit the attacking methods and attacking chances against the TOE or assets, by an unspecified large number of threatening agents. A.PHYSICAL can be realized, because, owing to the OE.PHYSICAL measures, the TOE machine administrator installs the TOE installed MFPs at places where room entrance/exit management is being executed, and where only people associated with the TOE are able to use it, and the attacking methods and attacking chances by an unspecified large number of threatening agents are limited.

A.ADMIN

A.ADMINISTRATOR requires that the TOE machine administrator is a reliable person, and that he/she will not do anything dishonest. A.ADMIN can be realized, because, owing to OE.ADMIN measures, the organization that is going to install the TOE selects an appropriate person who will execute his/her assigned role faithfully and who will do no wrong, for the TOE machine administrator, in order not to have the TOE machine administrator doing any dishonesty.

A.CE

A.CE requires that the person in charge of service for the TOE (a person accepted by KYOCERA MITA) will not do anything dishonest. A.CE can to be realized, because, owing to OE.CE measures, the TOE machine administrator will always be present at occasions when the person in charge of service conducts maintenances, etc., in order not to have the person in charge of service for the TOE doing any dishonesty.

8.2. Security Requirements Rationale

8.2.1. Compatibility of Security Function Requirements for Security Objectives

The support of TOE security function requirements for the security objectives are indicated in "Table 8-3　Security Objectives and TOE Security Function Requirements Support".

Table 8-3　Security Objectives and TOE Security Function Requirements Support

TOE Security Function Requirements \ Security Objectives		O.REMAIN	O.METHOD
TOE Security Function Requirements	FIA_UAU.2		X
	FIA_UAU.7		X
	FIA_UID.2		X
	FIA_SOS.1		X
	FDP_RIP.1	X	
	FMT_MTD.1		X
	FMT_MOF.1	X	X
	FMT_SMR.1		X
	FMT_SMF.1		X
	FPT_RVM.1	X	X

The rationales for "Table 8-3　Security Objectives and TOE Security Function Requirements Support" are indicated in the following.

O.REMAIN

It is possible to assure that information deleted from HDDs will never be accessed again, with the "subset residual information protection" policy of FDP_RIP.1.

The role of executing the HDD overwriting function is given to the TOE machine administrator, by FMT_MOF.1.

It is also possible to have FDP_RIP.1、FMT_MOF.1 executed without bypasses, with FPT_RVM.1.

With this, O.REMAIN, which is for preventing the printing/browsing of residue data, will become possible to be realized.

O.METHOD

First of all, a proper and approved TOE machine administrator is identified and authenticated by FIA_UID.2 and FIA_UAU.2. At this point, dummy characters (*) with the same length as the inputted characters will be displayed by FIA_UAU.7, to keep the TOE administrator management code secret. The TOE machine administrator is given the role of deciding the behavior of the overwriting method of the HDD overwriting function, by FMT_MOF.1. This role is always given to an appropriate TOE machine administrator, by FMT_SMR.1. The ability to enquire or modify the TOE administrator management code, which is TSF data, is restricted to only the TOE machine administrator, by FMT_MTD.1. It is also verified that the metric for authentication is a number with a fixed length of 8 figures, by FIA_SOS.1.

It is also possible to specify the management of the TOE administrator management code with FMT_SMF.1, and to have FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_SOS.1, FMT_MTD.1, and FMT_MOF.1 always executed without bypasses with FPT_RVM.1.

With the measures taken above, it will become possible to realize O.METHOD for sure, by limiting the authority to change the overwiting method of the HDD overwriting function to either the 3-time Overwrite method or the Once Overwrite method, to the TOE machine administrators.

8.2.2. Rationale for TOE security functional requirement dependencies

The dependent Relationships between the TOE security function requirements are indicated in "Table 8-4　Dependent Relationships Between TOE Security Function Requirements."

Table 8-4　Dependent Relationships Between TOE Security Function Requirements

No.	TOE Security Function Requirements	Hierarchical to	Dependent Relationships	Ref. No.	Note
1	FIA_UAU.2	FIA_UAU.1	FIA_UID.1	3	The dependency is satisfied, because FIA_UID.2 is an upper component of FIA_UID.1.
2	FIA_UAU.7	None	FIA_UAU.1	1	The dependency is satisfied, because FIA_UAU.2 is an upper component of FIA_UAU.1.
3	FIA_UID.2	FIA_UID.1	None	―	
4	FIA_SOS.1	None	None	―	

5	FDP_RIP.1	None	None	—	
6	FMT_MTD.1	None	FMT_SMR.1 FMT_SMF.1	8 9	
7	FMT_MOF.1	None	FMT_SMR.1 FMT_SMF.1	8 9	
8	FMT_SMR.1	None	FIA_UID.1	3	The dependency is satisfied, because FIA_UID.2 is an upper component of FIA_UID.1.
9	FMT_SMF.1	None	None	—	
10	FPT_RVM.1	None	None	—	

8.2.3. Mutual Effect of TOE Security Functional Requirements

The relationship of the mutual effect of security requirements will be verified in the following. The relationship of the mutual effect of security requirements is indicated in "Table 8-5 Mutual effect of security requirements."

Table 8-5 Mutual effect of security requirements

Function Requirements	Requirement providing protection		
	Bypass	**Corruption**	**Deactivation**
FIA_UAU.2	FPT_RVM.1	N/A	N/A
FIA_UAU.7	FPT_RVM.1	N/A	N/A
FIA_UID.2	FPT_RVM.1	N/A	N/A
FIA_SOS.1	FPT_RVM.1	N/A	N/A
FDP_RIP.1	FPT_RVM.1	N/A	N/A
FMT_MTD.1	FPT_RVM.1	N/A	N/A
FMT_MOF.1	FPT_RVM.1	N/A	N/A
FMT_SMR.1	N/A	N/A	N/A
FMT_SMF.1	N/A	N/A	N/A
FPT_RVM.1	N/A	N/A	N/A

N/A: Not Applicable

Bypass

FPT_RVM.1

FIA_UAU.2, FIA_UAU.7, and FIA_UID.2, which are related to the identification and authentication of TOE machine administrators, cannot be bypassed, because they are always called out when TOE machine administrators are identified and authenticated.

FIA_SOS.1, which is related to the verification of secrets, cannot be bypassed, because it is always called out when TOE administrator management codes are changed.

FDP_RIP.1, which is related to the protection of user's data, cannot be bypassed, because it is always called out after image data that is spool-stored or stored for a long period is logically deleted, or after an HDD formatting function is executed by the TOE machine administrator.

FMT_MTD.1, which is related to the management of TSF data, cannot be bypassed, because it is always called out when TOE administrator management codes are changed.

FMT_MOF.1, which is related to the behaviour management of the security functions, cannot be bypassed, because the identification and authentication of the TOE machine administrator is always called out when the setting for the HDD overwriting method is changed.

Corruption

Since this TOE does not have a function to access residue data for all the users, there is no need to implement access control or information flow control. The only interface to the management functions is the TOE machine administrator interface, and there are no other subjects that will access the TSF or TSF data. Therefore, there is no need to consider the corruption of TSF by an unjust subject.

Deactivation

The TSF will not be deactivated, because there is no mechanism in this TOE to set the security function off.

8.2.4. Rationale for the level of the minimum strength of function for security objectives

Although it is also assumed that this TOE will be utilized by being installed on MFPs at offices and schools, and connected to the LAN or local ports, residue data within the MFPs cannot be read out from the network, via the LAN/local-ports. And since the MFPs will be installed at places where room entrance/exit management is executed, there will not be any unspecified large number of attackers, including attackers with a medium level or more attacking force, in the operating environment of the TOE. For this reason, the attacking force will be "low-level," and the level of "the minimum strength of function" that can cope with this should be satisfied by a "SOF-basic."

8.2.5. Rationale for Assurance Requirements

This TOE will be utilized by being installed on MFPs, in offices or schools. However, since the users will not be an unspecified large number of people, and unjust actions will be attacks within the offices or schools, the attacking capability concerning the exposure of image data will be at a low level. For this reason, the selection of EAL3, which is a level sufficient for commercial MFPs, should be appropriate.

In addition, there are no specific assurance measures that will exceed EAL3.

8.3. TOE Summary Specification Rationale

8.3.1. Conformity of Security Functional Requirements for TOE Summary Specifications

The relationship of the security function requirements conforming to the TOE summary specifications is indicated in "Table 8-6　TOE Summary Specifications and Security Function Requirements Support".

Table 8-6　TOE Summary Specifications and Security Function Requirements Support

TOE Summary Specifications / TOE Security Function Requirements	SPF.AGAIN	SPF.ADMIN
FIA_UAU.2		X
FIA_UAU.7		X
FIA_UID.2		X
FIA_SOS.1		X
FDP_RIP.1	X	
FMT_MTD.1		X
FMT_MOF.1		X
FMT_SMR.1		X
FMT_SMF.1		X
FPT_RVM.1	X	X

The rationales for "Table 8-6　TOE Summary Specifications and Security Function Requirements Support" are indicated in the following.

FIA_UAU.2

The security function requirement FIA_UAU.2 that prescribes the behaviour of "user authentication before actions" is satisfied, because the security function SPF.ADMIN ("administrator authenticating function") always executes authentication when functions permitted to TOE machine administrators are accessed.

FIA_UAU.7

The security function requirement FIA_UAU.7 that prescribes the behaviour of "feedback of protected authentication" is satisfied, because the security function SPF.ADMIN ("administrator authenticating function") displays only dummy characters (*) with the same length as the characters inputted, on the operation panel, during the authentication.

FIA_UID.2

The security function requirement FIA_UID.2 that prescribes the behaviour of "user identication before actions" is satisfied, because, with the security function SPF.ADMIN ("administrator authenticating function"), the accessing person is always identified that he/she is a TOE machine administrator when functions permitted to TOE machine administrators are accessed, by requiring the TOE administrator management code.

FIA_SOS.1

The security function requirement FIA_SOS.1 that prescribes the behaviour of "verification of secrets" is satisfied, because the security function SPF.ADMIN ("administrator authenticating function") conducts the verification of the quality metric of the TOE administrator management code with the defined constitution.

FDP_RIP.1

The security function requirement FDP_RIP.1 that prescribes the behaviour of "subset residual information protection" is satisfied, because the security function SPF.ADMIN ("administrator authentication function") conducts not only the logical deletion but also the overwiting of the actual data area when image data files on the HDDs of the main board and printer board are to be deleted, and also conducts the overwriting of the whole disk when the TOE machine administrator executes an HDD formatting function.

FMT_MTD.1

The security function requirement FMT_MTD.1 that prescribes the behaviour of the "TSF data management" is satisfied, because the security function SPF.ADMIN ("administrator authenticating function") permits only the TOE machine administrator to display and change the TOE administrator management code setting of the TOE machine administrator.

FMT_MOF.1

The security function requirement FMT_MOF.1 that prescribes the behaviour of the "security functions" is satisfied, because the security function SPF.ADMIN ("administrator authenticating function") permits the role of changing the setting for the overwriting method in the PSF.AGAIN ("HDD overwriting function") to the 3-time Overwrite method or the Once Overwrite method, and the role of executing the HDD formatting function that initializes the whole HDD, to only the TOE machine administrators.

FMT_SMR.1

Roles are maintained upon the TOE machine administrators, because the security function SPF.ADMIN ("administrator authenticating function") conducts the identification and authentication of TOE machine administrators securely, and permits only TOE machine administrators to change TOE administrator management codes. It is also possible to relate a person succeeding in being identified and authenticated, to the role as a TOE machine administrator. With this, the security function requirement FMT_SMR.1 that prescribes the behaviour of security roles is satisfied.

FMT_SMF.1

FMT_SMF.1 has the ability to administer the TOE administrator management code with SPF.ADMIN ("administrator authenticating function"), which is a control point of FIA_UAU.2.

The protected authentication feedback is a fixed set of dummy figures, and there is no control item for FIA_UAU.7. The TOE machine administrators are the only identification targets, even for user identifications before actions, and since the TOE identifies the TOE machine administrators by having them conduct an operation designated for administrators, there is no control item for FIA_UID.2. There is also no control item for FIA_SOS.1, for the verification metric of secrets, because it is a number with a fixed length of 8 figures. There is also no control item for FDP_RIP.1, for the subset residual information protection, because residual information protection is implemented only upon the release of assignments, and the timing is fixed. There is also no control item for FMT_MTD.1 and FMT_MOF.1, because the only role group that mutually affects the TSF functions and TSF data are the TOE machine administrators, and there is no need for control. There is no control item for FMT_SMR.1, because the only users that form a portion of the role are the TOE machine administrators, and there is no need for control.

With this, the security function requirement FMT_SMF.1 that prescribes the behaviour of "specifying the management function" is satisfied, by installing SPF.ADMIN ("administrator authenticating function").

FPT_RVM.1

The security function requirement FPT_RVM.1 that prescribes the behaviour of "non-bypassability of the TSP" is satisfied, because the security function SPF.ADMIN ("administrator authenticating function") and PSF.AGAIN ("HDD overwriting function") are always executed without being bypassed.

8.3.2. Rationale for Security Functions Strength

In "6.3 Security Strength of Function," it claims SOF-basic for the security mechanism in the administrator authenticating function. On the other hand, it claims SOF-basic for the minimum strength of function of TOE, in "5.3 Minimum Strength of Function." Therefore, the strength of function is consistent in both of the cases, and SOF-basic for the security strength of function is appropriate.

8.3.3. Rationale for Assurance Measures

We will verify the effectiveness of the "6.4 Assurance Measures," in this section.

As indicated in Table 6-2, all the TOE security assurance requirements are made to correspond with document sets indicated in the "assurance measures" field.

The documents indicated in the assurance measures field cover the evidence required by the TOE security assurance requirement EAL3, prescibed by this ST.

◆ ACM_CAP.3 CM capabilities

[Assurance Measures] • KM-8030/KM-6030 Planning sheet for configuration management

• KM-8030/KM-6030 Rule sheet for configuration management

• KM-8030/KM-6030 Configuration list for the overseas versions

[Content] It prescribes the naming rules for identifying the TOE version, a list of the elements, and a unique identification of the elements, and also assures the modification of the TOE, and the maintenance of the completeness of the TOE.

◆ ACM_SCP.1 TOE CM coverage

[Assurance Measures] • KM-8030/KM-6030 Planning sheet for configuration management

• KM-8030/KM-6030 Rule sheet for configuration management

[Content] It prescibes the management method for changes, which accompany appropriate approvals for the elements that have been identified in the element list.

◆ ADO_DEL.1 Delivery procedures

[Assurance Measures] • KM-8030/KM-6030 Delivery procedure manual

[Content] It prescribes the means, equipment, and procedures that will be used for maintaining the security of the TOE, for the period until the Data Security Kit (B) hardware key, which is for activating the TOE, is delivered to the user from the developer.

◆ ADO_IGS.1 Installation, generation, and start-up procedures

[Assurance Measures] • Data Security Kit (B) Operation Guide
• INSTALLATION GUIDE for Data Security Kit (B)
• Printing System (V) Operation Guide Set-up Edition
• Scan System (G) Operation Guide Set-up Edition
• 8030/6030 SERVICE MANUAL

[Content] It prescribes the procedure and checking method for the TOE to conduct the installation/start-up in a secure way.

◆ ADV_FSP.1 Informal functional specification

[Assurance Measures] • KM-8030/KM-6030 Function specification sheet

[Content] It describes a detailed content of the behaviours of all the TOE security functions, and the external interface that is seen from the TOE machine administrators, or the TOE users.

◆ ADV_HLD.2 Security enforcing high-level design

[Assurance Measures] • KM-8030/KM-6030 High-level designing sheet

[Content] The functional specification of the TOE is fractionalized into more details as subsystems, and the purposes and functions are described and the security functions are identified, for each of the subsystems. The mutual relationships between the subsystems are also defined.

◆ ADV_RCR.1 Informal correspondence demonstration

[Assurance Measures] • KM-8030/KM-6030 Function support list

[Content] It describes the complete conformance at each of the levels of the TOE security functions (summary specification / functional specification / high-level design).

◆ AGD_ADM.1 Administrator guidance

[Assurance Measures] • Data Security Kit (B) Operation Guide

[Content] It describes the management functions and interfaces that the TOE machine administrators can utilize, and also describes the assumptions, etc. about user behaviours that will be associated to a secure operation of the TOE.

◆ AGD_USR.1 User guidance

[Assurance Measures] • Data Security Kit (B) Operation Guide

- 6030/8030 Operation Guide
- 6030/8030 Advanced Operation Guide
- Printing System (V) Operation Guide Function Edition
- Printing System (V) Operation Guide Set-up Edition
- Scan System Operation Guide Function Edition
- Scan System (G) Operation Guide Set-up Edition

[Content] It describes the security functions and interfaces that the TOE users can utilize, and also describes the using-methods including warnings, and guidelines, for a secure operation of the TOE.

◆ ALC_DVS.1 Identification of security measures

[Assurance Measures] • KM-8030/KM-6030 Regulation sheet for development security

[Content] It prescibes the physical, procedure-like, human, and other security measures that are used in the development environment, for the protection of TOE.

◆ ATE_COV.2 Analysis of coverage

[Assurance Measures] • KM-8030/KM-6030 Analysis sheet for the coverage test

[Content] It describes the sufficiency/completeness of the TOE security function tests.

◆ ATE_DPT.1 Testing: high-level design

[Assurance Measures] • KM-8030/KM-6030 High-level designing test specification

[Content] It provides an assurance for the TOE security function tests, from the normal operation of its inner mechanism.

◆ ATE_FUN.1 Functional testing

[Assurance Measures] • KM-8030/KM-6030 Functional test specification sheet

It provides an assurance for the TOE security function tests, by satisfying the security function requirements.

◆ ATE_IND.2 Independent testing - sample

[Assurance Measures] • TOE

[Content] It provides a reproduction of the environment for the TOE security function tests, and the testing materials.

◆ AVA_MSU.1 Examination of guidance

[Assurance Measures] • Data Security Kit (B) Operation Guide

- 6030/8030 Operation Guide
- 6030/8030 Advanced Operation Guide
- Printing System (V) Operation Guide Function Edition
- Printing System (V) Operation Guide Set-up Edition
- Scan System Operation Guide Function Edition
- Scan System (G) Operation Guide Set-up Edition

[Content] It describes the assumptions for the using-methods and operation of the TOE, so that there will be no danger of TOE machine administrators or TOE users changing the TOE security functions to an unsecure state, due to improper use.

◆ AVA_SOF.1 Strength of TOE security function evaluation

[Assurance Measures] • KM-8030/KM-6030 Analysis sheet of vulnerability

[Content] It describes the analysis of the "strength of TOE security function" for the security mechanism, by the TOE security function.

◆ AVA_VLA.1 Developer vulnerability analysis

[Assurance Measures] • KM-8030/KM-6030 Analysis sheet of vulnerability

[Content] It describes the fact that the vulnerability of the security functions will not be able to be abused, in an environment intended by TOE.

8.4. PP Claims Rationale

There is no conformance to a PP in this ST.

(Last page)