bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Control Software

Security Target

This document is a translation of the evaluated and certified security target written in Japanese.

Version: 1.03

Issued on: August 5, 2009

Created by: KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

<Revision History >

Date	Ver.	Approved	Checked	Created	Division	Revision
Jan. 6, 2009	1.00	Hirota	Ideyama	Atsumi	Development Division 12	Initial Version
Jun. 17, 2009	1.01	Hirota	Tada	Atsumi	Office Software Development Division 1	Deal with typos
Jun. 22, 2009	1.02	Hirota	Tada	Atsumi	Office Software Development Division 1	Deal with typos
Aug. 5, 2009	1.03	Hirota	Tada	Atsumi	Office Software Development Division 1	Deal with typos

— [Contents] ——————————————————————————————

— [List of Figures] ———————————————————————

— [List of Tables] ———————————————————————

1. ST Introduction

1.1. ST Identification

- ST Title	:	bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Control Software Security Target
- ST version	:	1.03
- Created on	:	August 5, 2009
- Created by	:	KONICA MINOLTA BUSINESS TECHNOLOGIES, INC. Kazuyuki Atsumi

1.2. TOE Identification

- TOE Name	:	Japanese Name : bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Zentai Seigyo Software English Name : bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 Control Software
- TOE version	:	A11U-0100-G10-06
- TOE type	:	Software
- Created by	:	KONICA MINOLTA BUSINESS TECHONOLOGIES, INC

1.3. TOE Overview

This paragraph explains the type, usage, main security functions, and operational environment of TOE.

1.3.1. TOE Type

bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 control software, which is the TOE, is an embedded software product installed in the flash memory on the MFP controller to control the operation of the whole MFP.

1.3.2. Usage of TOE and Main Security Functions

bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221 are digital multi-function products provided by Konica Minolta Business Technologies, Inc. composed by selecting and combining copy, print, scan and FAX functions. (Hereafter all the products are referred to as MFP") TOE is the "control software for bizhub 350 / bizhub 250 / bizhub 200 / bizhub 362 / bizhub 282 / bizhub 222 / ineo 362 / ineo 282 / ineo 222 / VarioLink 3621 / VarioLink 2821 / VarioLink 2221"

that controls the entire operation of MFP, including the operation control processing and the image data management triggered by the panel of the main body of MFP or through the network.

TOE supports the protection from exposure of the highly confidential document stored in the MFP. Moreover, for the danger of illegally bringing out HDD, which stores image data in MFP, TOE provides the protection function to overwrite at once the data that became unnecessary and the protection function using HDD lock function installed in HDD. TOE can encrypt image data written in HDD by installing the encryption board which is the oprional part of MFP. Besides, TOE has a deletion method compliant with various overwrite deletion standards. It deletes all the data of HDD completely and it contributes to the prevention of information leakage of the organization that uses MFP by using this method at the time of abandonment or the lease returns.

1.4. TOE Description

1.4.1. Role of TOE Users

The roles of the personnel related to the use of MFP with TOE are defined as follows.

- User
  An MPF user who copys, scans, etc. with MFP.(In general, the employee in the office is assumed.)

- Administrator
  An MFP user who manages the operations of MFP. Manages MFP's mechanical operations and user boxes. In general, it is assumed that the person elected from the employees in the office plays this role.)

- Service Engineer
  A user who manages the maintenance of MFP. Performs the repair and adjustment of MFP. (In general, the person-in-charge of the sales companies that performs the maintenance service of MFP in cooperation with Konica Minolta Business Technologies Inc. is assumed.)

- Responsible person of the organization that uses the MFP
  A responsible person of the organization that manages the office where the MFP is installed. Assigns an administrator who manages the operation of MFP.

- Responsible person of the organization that manages the maintenance of MFP
  A responsible person of the organization that manages the maintenance of MFP. Assigns service engineers who manages the maintenance of MFP.

Besides this, though not a user of TOE, those who go in and out in the office are assumed as an accessible persons to TOE.

1.4.2. Physical Scope of TOE

1.4.2.1. Use Environment

Figure 1 shows a general environment in which the usage of MFP equipped with TOE is expected. Moreover, the matters expected to occur in the use environment are listed below.

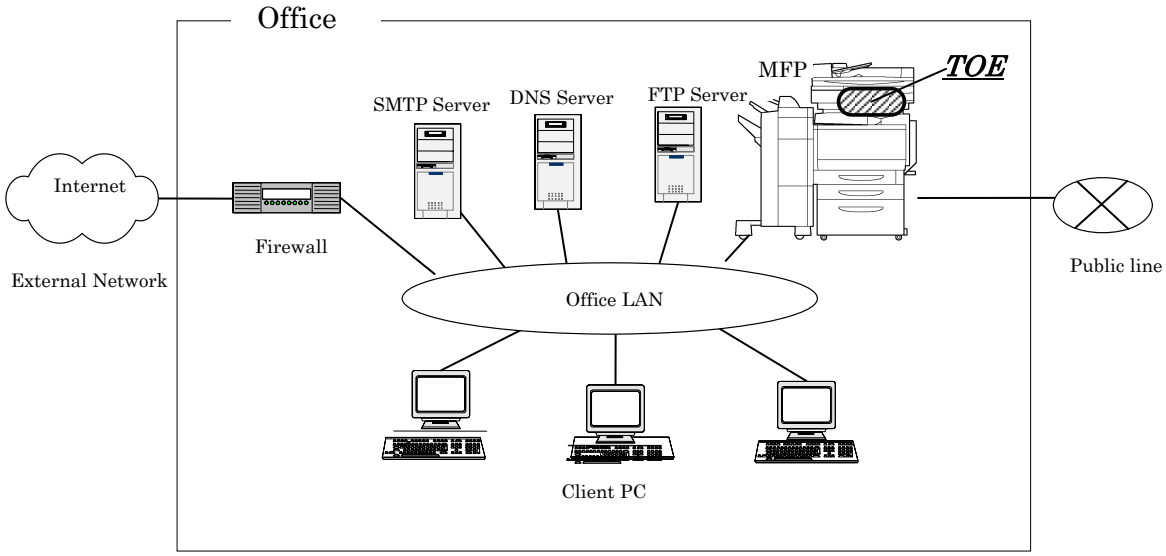

Figure 1　An example of MFP's use environment

- An intra-office LAN exists as a network in the office.
- MFP is connected to the client PCs via the intra-office LAN, and has mutual data communications.
- When a SMTP or FTP server is connected to the intra-office LAN, MFP can carry out data communications with these servers, too. (The DNS service will be necessary when setting a domain name of SMTP or FTP server.)
- When the intra-office LAN connects to an external network, measures such as connecting via a firewall are taken, and an appropriate setup to block access requests to the MFP from the external network is applied.
- The intra-office LAN provides a network environment that cannot be intercepted by the office operations including using switching hubs and installing wiretapping detectors.
- The public line connected with MFP is used for communications by FAX and the remote support function.

1.4.2.2. Operation Environment

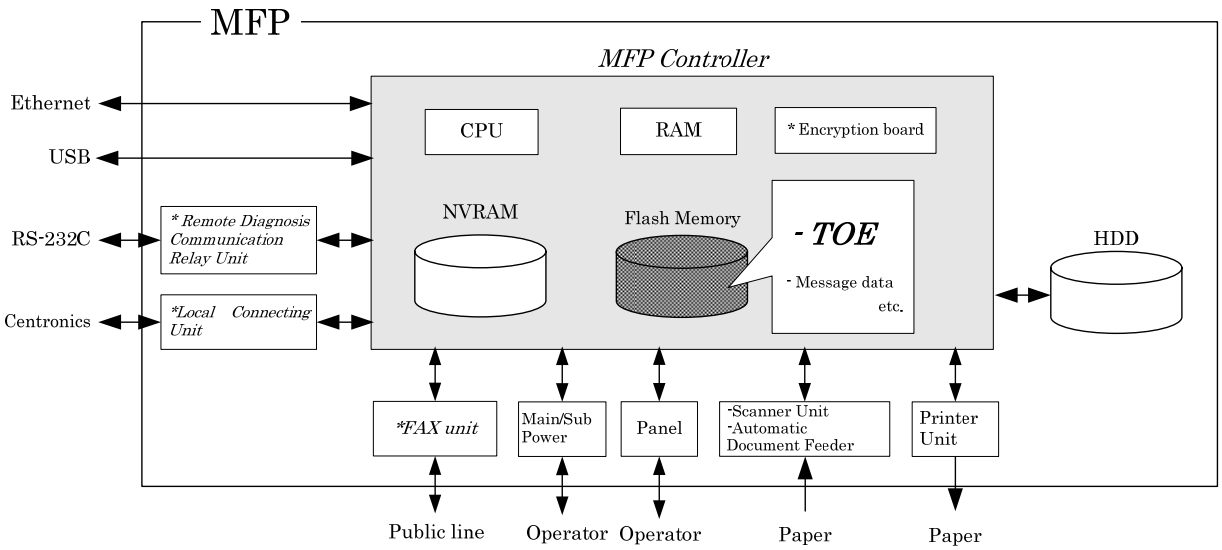

Figure 2 Hardware composition relevant to TOE

Figure2 shows the structure of the hardware environment on the MFP that TOE needs for the operation. The MFP controller is installed in the main body of MFP, and TOE exists in the flash memory on the MFP controller, loaded into the main memory.

The following explains about the unique hardware on the MFP controller, the hardware having interfaces to the MFP controller, and the connection using RS-232C, shown in Figure 2.

- Flash memory
  A storage medium that stores the object code of the "MFP Control Software" which is the TOE. Additionally, stores the message data expressed in each country's language to display the response to access through the panel and network.

- RAM
  A volatile memory. This memory medium stores image data.

- NVRAM
  A nonvolatile memory. This memory medium stores various settings that MFP needs for the operation. (administrator password, transmission address data, etc)

- Encryption board (*optional part)
  Implemented the encryption function for enciphering all data written in HDD. An integrated circuit for encryption. Is not pre-installed in MFP as a standard function according to the circumstances in sales, but sold as an optional part.

- Panel
  An exclusive control device for the operation of MFP, equipped with a touch panel of a liquid crystal monitor, ten-key, start key, stop key, screen switch key, etc.

- Ethernet

Supports 10BASE-T, 100BASE-TX, and Gigabit Ethernet.

- USB
  Port for the print by local connection

- Scan unit / auto document feeder
  A device that scans images and photos from paper and converts them into digital data.

- Printer unit
  A device to actually print the image data which were converted for printing when receives a print request from the MFP controller.

- HDD (*optional part)
  Hard disk drive. This is used not only for storing image data as files but also as an area to swap image data that exceeds RAM processing capacity.
  As a feature function, security function (HDD lock function) is installed, being possible to set a password and not being possible to read and write unless it agrees to the password. Furthermore, when the frequency of uniformity of it becomes unsuccessful in password collation, the function is also ready to lock the password collation function.
  Is not pre-installed in MFP as a standard function according to the circumstances in sales, but sold as an optional part. The function which needs HDD (1.4.3.3 User Box function) cannot be used without its option.

- FAX Unit (*optional part)
  A device used for communications for FAX-data transmission and remote diagnostic (described later) via the public line. Is not pre-installed in MFP as a standard function according to the circumstances in sales, but sold as an optional part.

- Local Connecting Unit (*optional part)
  Unit for using the printer function with local connection by connecting to the client PC with centronics interface (parallel port). Is not pre-installed in MFP as a standard function according to the circumstances in sales, but sold as an optional part.

- Remote diagnostic communication relay unit (* optional part)
  It enables to connect serially via RS-232C. By connecting to the modem that is connected to the public line, the remote diagnostic function (described later) via this interface can be used when any troubles occurred. Is not pre-installed in MFP as a standard function according to the circumstances in sales, but sold as an optional part.

1.4.2.3. Guidance

- bizhub 350 / 250 / 200 Service Manual [Security Function] (Japanese)
- bizhub 362 / 282 / 222 / ineo 362 / 282 / 222 / VarioLink 3621 / 2821 / 2221 SERVICE MANUAL [SECURITY FUNCTION] (English)
- bizhub 350 / 250 / 200 User's Guide [Security Function] (Japanese)
- bizhub 362 / 282 / 222 User's Guide [Security Operations] (English)
- ineo 362 / 282 / 222 User's Guide [Security Operations] (English)

- VarioLink 3621 / 2821 / 2221 User's Guide [Security Operations] (English)

1.4.3. Logical Scope of TOE

Users use a variety of functions of TOE from the panel and a client PC via the network. Hereafter, this section explains typical functions, such as the basic function, the user box function to manage the image files stored, the administrator function manipulated by administrator, the service engineer function manipulated by service engineer, and the function operated in the background without user's awareness.

1.4.3.1. Basic Function

In MFP, a series of functions for the office work concerning the image such as copy, print, scan, and fax exists as basic functions, and TOE performs the core control in the operation of these functions. It converts the raw data acquired from the external device of the MFP controller into the image files, and registers them in RAM and HDD. (For print image files from PCs, multiple types of conversion are applied.) The image files are converted into data to be printed or sent, and transmitted to the device outside of the MFP controller concerned.

Operations of copy, print, scan, and FAX are managed by the unit of job, so that such operations can be aborted, by giving directions from the panel.

The following is the functions related to the security in the basic function.

- Secure Print Function

  When a secure print password is received together with printing data, the image data is stored as standby status in RAM. Then, printing is performed by a print direction and password entry from the panel.

  When printing is requested by a client PC, this function eliminates the possibility that other users stole a glance at the printing of highly confidential data, or such data is slipped into the other printings.

1.4.3.2. User Choice Function

User can freely set, including image quality adjustment (magnification and print density, etc.) which are chiefly needed to use the basic function, a standard layout, the power saving shift time, and the auto reset time (function that the display of the operation panel returns to a basic screen if it doesn't operate it during the fixed time).

1.4.3.3. User Box Function

A directory called a "user box" can be created as an area to store image files in HDD. Two types of user box are usable; the one is the public user box which all users can use and the other is the user box used by setting password which can be used individually or among users with sharing password.

TOE processes the following operation requests to a user box or image files in the user box from the panel or the network unit through a network from a client PC.

- Print, transmit, and download from a client PC, of image files in a user box
- Delete an image file in a user box
- Set a storing period of image files in a user box (delete automatically after the period passes.)
- Change the name, user box ID and password of a user box, or delete a user box and so on.

If HDD is not installed, a "user box" cannot be created.

1.4.3.4. Administrator Function

TOE provides the functions such as the management of user boxes and management of various settings of the network, image quality, etc in the administrator mode that only authenticated administrator can manipulate.

The following shows the functions related to the security.

- Management of user box settings
  - Chang of user box IDs
  - Change of user box password
- Management of network settings
  - Connection setting of the intra-office LAN (setting of DNS server)
  - SMTP setting (setting of the SMTP server utilized by E-mail transmission)
  - IP addresses, NewBIOS names, and AppleTalk printer names etc.
- Overwrite delete function at the time of disposal
  - Perform the overwrite deletion for the whole data area of HDD
  - Initialize the various settings and the charging information in NVRAM that administrators set.

The followings below are the operation setting functions related especially to the behavior of the security function.

- Setup of a password policy function
  - It is selected whether to enable or disable the function to check the several conditions of the password, such as the number of valid digits of various passwords.
- Setup of the prohibit function of authenticating operations
  - The function detecting unsuccessful authentication in each authentication function
  - The above-mentioned operational modes are selected
  - With the unsuccessful authentication detection mode, the user box password matching function works when downloading user box files by PCs.
- Setup the method of the remaining information overwrite deletion function (described later)
  - Overwrite data : Valid or invalid setting of the method of 0x00 → 0x00 → 0x00 exists.
  - Whether to activate or stop the above operational method is selected
- Setup of the HDD lock function
  - Wether to activate or stop the function is selected
  - HDD lock password is registered or changed when the function is activated
- Setup of the encryption function (*only when the encryption board is installed)
  - Whether to activate or stop the function is selected
  - An encryption key passphrase is registered or changed when the function is activated.

1.4.3.5. Service Engineer Function

TOE provides a management function of administrator and a maintenance function, such as adjusting the device for Scan/Print etc, within the service mode that only a service engineer can operate. The following shows the functions related to the security.

- Initialization of the administrator mode password
- Setup of the remote diagnostic function (described later)
- Total clear function
  - Initialize the various settings that administrators set
- Memory dump function
  - Function to confirm the NVRAM condition when troubles happened.
  - Possible to confirm the value of administrator password etc. by dumping

1.4.3.6. Other Functions

TOE provides the functions that run background without awareness of the user and the updating function of TOE. The following explains the major functions.

(1) Overwrite delete function of the remaining information
It performs the overwrite deletion of the unneeded image files made by the job termination, the deleting operation by the job management function, the deletion of image files stored in the user box, and the deletion after a lapse of the storage period of image files. Overwriting data is 0x00 → 0x00 → 0x00 and performs the overwriting in this order.

(2) Remote diagnostic function
MFP's equipment information such as operating state, setting information of administrator password and the number of printed sheets is managed by making use of multiple connection methods such as E-mail, FAX unit, and a modem connection through the RS-232C to communicate with the support center of MFP managed by Konica Minolta Business Technologies, Inc. In addition, if necessary, appropriate services (shipment of additional toner packages, account claim, dispatch of service engineers due to the failure diagnosis, etc.) are provided.

(3) Updating function of TOE
TOE facilitated with the function to update itself. When it receives command from the remote diagnostic function, there is a method to download from FTP server through Ethernet and can update. Also, there is a method that performs by the connection of the compact flash memory medium.

(4) Encryption key generation function
Performs encryption/decryption by encryption board when writing data in HDD or reading data from HDD, if the encryption board which is the optional part is installed in MFP controller. (TOE does not process the encryption and description itself.)
The operational setup of this function is performed by the administrator function. When activated, TOE generates the encryption key by the encryption key passphrase that was entered on the panel.

TOE makes the full use of the security function (encryption function) of encryption board, which is an external entity. The following explains typical functions related to the external entity.

(5) Utilization of HDD lock function

HDD, an external entity, activates the HDD lock function as a function to protect unauthorized bring-out of data and so on when a password is set up.

The administrator function does the operation setting of this function. As for the starting operation of MFP, the access to HDD is permitted by the matching of the HDD lock password set to the HDD and the one set on the MFP. (Even if HDD is bring out, it is impossible to use it excluding the MFP that the concerned HDD installed.)

(6) Utilization of encryption board

Eencryption board, an external entity, activates a function to encrypt the data in HDD as a function to protect unauthorized bring-out of data and so on when an encryption key passphrase is set up.

1.4.3.7. Enhanced Security Function

Various setting functions related to the behavior of the security function for the Administrator function and the Service engineer function can be set collectively to the secure values by the operation settings of the "Enhanced Security Function". Each value set is prohibited changing itself into the vulnerable one individually. As the function that does not have a setting function of the operation individually, the setting of the secure print authentication function exists, but it is the setting to enhance the security. (operation method that inputting password into after having chosen ID)

The following explains the series of the setting condition of being the enhanced security function active. In order to activate the enhanced security function, the prerequisite is required that an administrator password and a service code should be set along with the password policy.

- Setup of password policy function : Valid
- Setup of the network setting modification function with SNMP (v1, v2, and v3) : Prohibited
- Setup of secure print authentication method : Operation of password examination after the file ID is specified
- Setup of prohibition function of authentication operation : Valid (account lock status (threshold of unsuccessful attempts: 3). The user box authentication method becomes password examination function operating method when downloading.)
- Setup of HDD lock function : Valid (If encryption function is activated, this can be set invalid.)
- Setup of encryption function : Valid (If HDD lock function is activated, this can be set invalid.)
- Setup of overwrite delete function for the remaining information : Valid
- Total clear function : Prohibited
- Memory dump function : Prohibited

● Remote diagnostic function[1]	: - Prohibited connecting RS232C modem - Prohibited receiving function by connecting FAX unit - Prohibited receiving function by e-mail

[1] However, the transmission function connecting FAX unit and the transmission function by E-mail are activated.

2. Conformance Claims

2.1. CC Conformance Claim

This ST conforms to the following standards.

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model 2006/9 Version 3.1 Revision 1 (Translation v1.2)
Part 2: Security functional requirements 2007/9 Version 3.1 Revision 2 (Translation v2.0)
Part 3: Security assurance requirements 2007/9 Version 3.1 Revision 2 (Translation v2.0)

- Security function requirement : Part2 Extended
- Security assurance requirement : Part3 Conformant

2.2. PP Claim

There is no PP that is referenced by this ST.

2.3. Package Claim

This ST conforms to Package: EAL3. There is no additional assurance component.

2.4. Reference

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2006 Version 3.1 Revision 1 CCMB-2006-09-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2007 Version 3.1 Revision 2 CCMB-2007-09-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2007 Version 3.1 Revision 2 CCMB-2007-09-003
- Common Criteria for Information Technology Security Evaluation: Evaluation methodology September 2007 Version 3.1 Revision 2 CCMB-2007-09-004

3. TOE Problem Definition

This chapter will describe the concept of protected assets, assumptions, threats, and organizational security policies.

3.1. Protected Assets

Security concept of TOE is "the protection of data that can be disclosed against the intention of the user". As MFP is generally used, the following image file in available situation becomes the protected assets.

- Secure Print File
  - Image files registered by the secure print
- User Box File
  - Image files stored in user box except "Public"

In the print of a secure print file, making in the preparation for the threat thought when unauthorized MFP is connected by any chance, the setting of MFP (IP address etc.) requires not to be modified illegally. Therefore, the setting of MFP (IP address etc.) is considered as subsidiary protected assets.

As for a image file of a job kept as a wait state by activities of plural jobs, and a image file of a job kept that prints the remainder of copies becoming as a wait state for confirmation of the finish, and other than the image file dealt with the above-mentioned is not intended to be protected in the general use of MFP, so that it is not treated as the protected assets.

On the other hand, when the stored data have physically gone away from the jurisdiction of a user, such as the use of MFP ended by the lease return or being disposed, or the case of a theft of HDD, the user has concerns about leak possibility of every remaining data. Therefore, in this case, the following data files become protected assets.

- All User Box Files
  - Image files stored in all types of user boxes including "Public" user box
- Swap Data Files
  - Files to constitute images that are generated by copy and PC print of big size that does not fit into an RAM area. (including secure print file).
- Overlay Image Files
  - Background image files
  - This registered image file can be set as wallpaper and used for copying, etc.
- HDD accumulation image files
  - Files stored in an HDD from PC print, and printed by the operation from panel
- Remaining Image files[2]

[2] This data is assets controlled by means of TOE installed so as not to be generated with the operation of the security function. The threat identification explains the treatment of these assets as an event that can happen when it is assumed that security objectives were unimplemented.

  - Files which remain in the HDD data area that is not deleted only by general deletion operation (deletion of a file management area)
- Transmission address data files
  - Files including an E-mail address, a phone number, etc.

3.2. Assumptions

The present section identifies and describes the assumptions for the environment for using the TOE.

A.ADMIN (Personnel conditions to be an administrator)

Administrators, in the role given to them, will not carry out a malicious act during the series of permitted operations given to them.

A.SERVICE (Personnel conditions to be a service engineer)

Service engineers, in the role given to them, will not carry out a malicious act during series of permitted operations given to them.

A.NETWORK (Network connection conditions for MFP)

- The intra-office LAN where the MFP with the TOE will be installed is not intercepted.
- When the intra-office LAN where the MFP with the TOE will be installed is connected to an external network, access from the external network to the MFP is not allowed.

A.SECRET (Operational condition about secret information)

Each password and encryption key passphrase do not leak out from each user in the use of TOE.

A.SETTING (Operational setting condition of Enhanced Security function)

MFP with the TOE is used after enabling the enhanced security function.

3.3. Threats

In this section, threats that are expected during the use of the TOE and the environment for using the TOE are identified and described. In the threats described below, T.BRING-OUT-STORAGE concerning HDD bring-out and T.ACCESS-BOX concerning the user box function that HDD is indispensable do not exist as threats if HDD is not installed.

T.DISCARD-MFP (Lease-return and disposal of MFP)

When leased MFPs are returned or discarded MFPs are collected, secure print files, user box files, on-memory image files, swap data files, overlay image files, HDD-remaining image files, transmission address data files, and various passwords which were set up can leak by the person with malicious intent when he/she analyzes the HDD or NVRAM in the MFP.[3]

[3] When HDD is not installed, only NVRAM transmission address data files and various passwords can leak.

T.BRING-OUT-STORAGE (An unauthorized carrying out of HDD)

- All user box files, swap data files, overlay image files, HDD accumulation image files, and remaining image files can leak by a malicious person or a user illegally when he/she brings out the files to analyze the HDD in a MFP.
- A person or a user with malicious intent illegally replaces the HDD in MFP. In the replaced HDD, newly created files such as user box files, swap data files, overlay image files, HDD accumulation image files, and remaining image files are accumulated. A person or a user with malicious intent takes out to analyze the replaced HDD, so that such image files will leak.

T.ACCESS-BOX (Unauthorized access to the user box which used a user function)

Exposure of the user box file when a person or a user with malicious intent accesses the user box where other user owns, and downloads, prints and transmits the user box file (E-mail transmission, FTP transmission, SMB[4] transmission).

T.ACCESS-SECURE-PRINT (Unauthorized access to the secure print file which used a user function)

Exposure of secure print file when a person or a user with malicious intent prints the secure print files that are not permitted to use.

T.UNEXPECTED-TRANSMISSION (Unauthorized change of network setting)

- Malicious person or user changes the network settings that are related to the transmission of a user box file. Even an addressee is set precisely, a user box file is transmitted (the E-mail transmission or the FTP transmission) to the entity which a user does not intend to, so that a user box file is exposed.

< The network settings which are related to user box file transmission>

- Setting related to the SMTP server
- Setting related to the DNS server

- Malicious person or user changes the network settings which set in MFP to identify MFP itself where TOE installed, by setting to the value of the entity such as another unauthorized MFP from the value of MFP (NetBIOS name, AppleTalk printer name, IP address etc) that TOE is originally installed, so that secure print files are exposed.

T.ACCESS-SETTING (An unauthorized change of a function setting condition related to security)

The possibility of leaking user box files and secure print file rises because those malicious including users changes the settings related to the enhanced security function.[5]

3.4. Organizational Security Policies

There is no organizational security policy assumed to be applied to this TOE.

[4] An Abbreviation of Server Message Block. A protocol to realize the file sharing and printer sharing on Windons

[5] When HDD is not installed, only secure print file can leak.

4. Security Objectives

In this chapter, in relation to the assumptions, the threats, and the organizational security policy identified in Chapter 3, the required security objectives policy for the TOE and the environment for the usage of the TOE are described by being divided into the categories of the security objectives for the TOE and the security objectives for the environment, as follows.

When an HDD is not installed, unnecessary security objectives may exist, but hereafter, assuming that an HDD was installed, this chapter disserts about the security objectives and the security requirements thought to be the maximum necessity against the threat.

4.1. Security Objectives for the TOE

In this section, the security objectives for the TOE is identified and described.

O.BOX (Access control for user boxes)

TOE permits only a user who was allowed to use that user box the user function of user box file in that user box.

O.SECURE-PRINT (Access control for secure print files)

TOE permits the print of the secure print file only to the user who was allowed to use the file.

O.CONFIG (Access limitation to management function)

TOE permits only the administrator the operation of the following functions.

- The setting function related to the SMTP server
- The setting function related to the DNS server
- The setting function related to the address of MFP
- The setting function of HDD lock function and encryption function
- The function related to the setting of Enhanced Security function

O.OVERWRITE-ALL (Complete overwrite deletion)

- TOE overwrites all the data regions of HDD in MFP with deletion data, and makes all image data unable to restore. In addition, TOE provides a function to delete transmission address data and a function to initialize settings such as the passwords on NVRAM (administrator passwords, HDD lock passwords, encryption key passphrase) set by a user or an administrator.

O.OVERWRITE-FILE (Overwrite deletion of each file)

When image files written in HDD in MFP becomes unnecessary, TOE overwrites the deletion data and makes those images unable to restore.

O.CRYPT-KEY (Encryption key generation)

TOE generates an encryption key to encrypt and store all the data written in the HDD in the MFP including image files.

O.CHECK-HDD (Validity confirmation of HDD)

TOE verifies that the correct HDD is set up.

O.CRYPTO-CAPABILITY (The support operation to utilize encryption function)

TOE supports necessary mechanical operations to utilize the encryption function by encryption board.

O.LOCK-HDD-CAPABILITY (The support operation to utilize HDD lock function)

TOE supports necessary mechanical operations to utilize the HDD lock function by HDD.

4.2. Security Objectives for the Operational Environment

In this section, the security objectives for the operational environment of TOE are described.

OE.CRYPTO (Utilization of encryption function)

When the encryption objectives of image files stored in HDD for the use of TOE is required to perform, administrator buys the lisence of the encryption board and sets the encryption of image files written in HDD in MFP by the encryption function of encryption board with the service engineer.

OE.LOCK-HDD (Utilization of HDD that has HDD lock function)

Service engineer and administrator install the HDD which had HDD lock function in MFP and set to use that function.

OE.FEED-BACK (Feedback of password)

The applications such as a browser, PC printer driver etc. that the administrator and user utilize by client PC to access MFP provide appropriate protected feedback to the secure print password, user box password, and administrator password, which will be entered.

OE.ADMIN (A reliable administrator)

The responsible person in the organization who uses MFP will assign a person who can faithfully execute the given role during the operation of the MFP with TOE as an administrator.

OE.SERVICE (The service engineer's guarantee)

- The responsible person in the organization managing the maintenance of MFP educates a service engineer in order to faithfully carry out the given role for the installation of the TOE, the setup of TOE and the maintenance of the MFP with TOE.
- The administrator observes the maintenance work of MFP with TOE by a service engineer.

OE.NETWORK (Network Environment in which the MFP is connected)

- The responsible person in the organization who uses MFP carries out the tapping prevention measures by setting the cipher communications equipment and the tapping detection equipment to the LAN of the office where MFP with TOE is installed.
- The responsible person in the organization who uses MFP carries out the measures for the unauthorized access from the outside by setting up the equipment such as the firewall to intercept the access from an external network to MFP with TOE.

OE.SECRET (Appropriate management of confidential information)

The administrator has the user implement the following operation.

- Keep the secure print password confidential.
- Keep the user box password confidential between the users who commonly utilize it.
- Should not set the value that can be guessed for the secure print password and the user box password.
- The user box password should be properly changed.
- When the administrator changes the user box password, make the user to change it promptly.

The administrator executes the following operations.

- Avoid setting an easy-to-guess value on the administrator password, HDD lock password, and encryption key passphrase.
- Keep the administrator password, HDD lock password, and encryption key passphrase confidential.
- Change the administrator password, HDD lock password, and encryption key passphrase appropriately.

The service engineer executes the following operations.

- Should not set the value that can be guessed for the service code.
- Keep the service code confidential.
- The service code should be properly changed.
- When the service engineer changes the administrator password, make the administrator to change it promptly.

OE.SESSION (Termination of session after operation)

The administrator has the user implement the following operation.

- After the operation of the functions for secure print files ends, the logoff operation is performed.
- After the operation of the functions for user box files ends, the logoff opearion is performed.

The administrator executes the following operation.

- After the operation of the various functions in administrator mode ends, the logoff operation is performed.

The service engineer executes the following operation.

- After the operation of the various functions in service mode ends, the logoff operation is performed.

OE.SETTING-SECURITY (Operational setup of Enhanced Security function)

- The administrator makes the setup of the enhanced security function effective for the operation of TOE.

4.3. Security Objectives Rationale

4.3.1. Necessity

The correspondence between the assumptions, threats and security objectives are shown in the following table. It shows that the security objectives correspond to at least one assumption or threat.

Table 1 Conformity of security objectives to assumptions and threats

Assumption/Treat / Security objectives	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	A.SETTING	T.DISCARD-MFP	T.BRING-OUT-STORAGE	T.ACCESS-BOX	T.ACCESS-SECURE-PRINT	T.UNEXPECTED-TRANSMISSION	T.ACCESS-SETTING
O.BOX								X			
O.SECURE-PRINT									X		
O.CONFIG										X	X
O.OVERWRITE-ALL						X					
O.OVERWRITE-FILE							X				
O.CRYPT-KEY							X				
O.CHECK-HDD							X				
O.CRYPTO-CAPABILITY							X				
O.LOCK-HDD-CAPABILITY							X				
OE.CRYPTO							X				
OE.LOCK-HDD							X				
OE.FEED-BACK								X	X	X	X
OE.ADMIN	X										
OE.SERVICE		X									
OE.NETWORK			X								
OE.SECRET				X							
OE.SESSION								X	X	X	X
OE.SETTING-SECURITY					X						

4.3.2. Sufficiency of Assumptions

The security objectives for the assumptions are described as follows.

- **A.ADMIN (Personnel Conditions to be an Administrator)**
  This condition assumes that administrators are not malicious.
  With OE.ADMIN, the organization that uses the MFP assigns personnel who are reliable in the organization that uses the MFP, so the reliability of the administrator is realized.

- **A.SERVICE (Personnel Conditions to be a Service Engineer)**
  This condition assumes the service engineer are not malicious.
  With OE.SERVICE, the organization that manages the maintenance of the MFP educates the service engineer. Also the administrator needs to observe the maintenance of the MFP, so that the reliability of service engineers is assured.

- **A.NETWORK (Network Connection Conditions for the MFP)**
  This condition assumes that there are no wiretapping activities for the intra-office LAN and no access by an unspecified person from an external network.
  OE.NETWORK regulates the wiretapping prevention by the installation of devices such as a wiretapping detection device and device to perform the encryption communication on the intra-office LAN. It also regulates the unauthorized access prevention from external by the installation of devices such as firewall in order to block access to the MFP from the external networks, so that this condition is realized.

- **A.SECRET (Operating condition concerning confidential information)**
  This condition assumes each password and encryption key passphrase using for the use of TOE should not be leaked by each user.
  OE.SECRET regulates that the administrator makes the user to execute the operation rule concerning the secure print password and user box password, and that the administrator executes the operation rule concerning the administrator password, HDD lock password and encryption key passphrase. It also regulates that the service engineer executes the operation rule concerning the service code, so that this condition is realized.

- **A.SETTING (Enhanced Security Function Operational Setup Condition)**
  This condition assumes the enhanced security function operational settings condition is satisfied.
  OE.SETTING-SECURITY regulates that this is used after the administrator activates the enhanced security function, so that this condition is realized.

4.3.3. Sufficiency of Threats

The security objectives against threats are described as follows.

- **T.DISCARD-MFP (Lease return and disposal of MFP)**
  This threat assumes the possibility of leaking information from the HDD in MFP collected from the user.

O.OVERWRITE-ALL is that TOE provides the function to overwrite data for the deletion of all data area of HDD and initializes the information of NVRAM, so that the possibility of the threat is removed by executing this function before MFP is collected.
Accordingly, this threat is countered sufficiently.

- **T.BRING-OUT-STORAGE (Unauthorised bring-out of HDD)**

This threat assumes the possibility that the image data in HDD leaks by being stolen from the operational environment under MFP used or by installing the unauthorised HDD and taking away with the data accumulated in it.
O.OVERWRITE-FILE is that TOE overwrites the deletion data when the image file written in HDD becomes unnecessary, and so the data available of the minimum requirement exist on HDD. Therefore, the threat is reduced greatly.
Also, the possibility of the threat is removed since the administrator selectes at least one measures from the following two objectives.

(1) O.CRYPTO-KEY assumes that TOE generates an encryption key to encrypt the data written in the HDD, a mechanical operation to use the encryption function is supported by O.CRYPTO-CAPABILITY, and the encryption function with encryption board with the administrator settings is used by OE.CRYPTO.
(2) By O.LOCK-HDD-CAPABILITY, a mechanical operation to use the HDD lock function is supported, and the setup to operate HDD lock function by administrator is performed by OE.LOCK-HDD. Then HDD lock function is activated.

By HDD is replaced and a HDD which doesn't have the function that assumes this measure is installed, the significant risk which leaks the data accumulated in the replaced HDD by taking it out exists. For this, O.CHECK-HDD verifies the validity of HDD set up by TOE and so no data is written in HDD replaced secretly.
Therefore, the possibility of the threat is removed.
Accordingly, this threat is countered sufficiently.

- **T.ACCESS-BOX (Unauthorised access to user box using user function)**

This threat assumes the possibility that an unauthorised operation is done by using the user function for the user box which each user uses to store the image file.
The operation of the user box file in a user box is limited only for the authorized user by O.BOX, and so the possibility of the threat is removed.
OE.FEED-BACK regulates to return the protected feedback for the entered password in the authentication of the user box password, so that O.BOX is supported sufficiently.
Accordingly, this threat is countered sufficiently.

- **T.ACCESS-SECURE-PRINT (Unauthorized access to a secure print file)**

This threat assumes the possibility that an unauthorized operation is done to the secure print.
The operations of the secure print are limited only to the authorized user by O.SECURE-PRINT, so that the possibility of the threat is reduced.
OE.FEED-BACK regulates to return the protected feedback for the entered password in the access authentication to the secure print, and OE.SESSION requires the log-off operation after the operation ends, so that O.SECURE-PRINT are supported sufficiently.
Accordingly, this threat is countered sufficiently.

- **T.UNEXPECTED-TRANSMISSION (Unauthorised change in network setting)**

This threat assumes the possibility of sending the user box file to the address that isn't intended, when the network setting that relates to the transmission is illegally changed. This is concerned about a possibility that the user box file is transmitted to the specified server illegally without the change of the network environment constitution by the malicious person by, for instance, illegally being changed the address of the SMTP server that relays E-mail for the E-mail, or illegally being changed the address of the DNS server where the domain name is inquired when the address of the SMTP server is used for a search of the domain name. For FTP transmission, by being likely to use the mechanism of the search of the domain name is concerned about the similar possibility of the incident might be occurred by E-mailing.
Furthermore, when the network setting which is related to the address of MFP is modified illegally, it assumes the possibility to use the print function to the unauthorized entity from client PC by the user who believes as TOE. Especially, it becomes a problem if a secure print file which is required to be concealed from other users in the office is transmitted to the unauthorized entity.
On the other hand, O.CONFIG regulates that the role to operate the network setting relating to the transmission of TOE is limited to the administrator, and so the possibility of this threat is removed.
OE.FEED-BACK regulates that the protected feedback is returned for the entered password by the administrator's authentication and OE.SESSION requires to logoff after the operation ends, so that O.CONFIG is supported sufficiently.
Accordingly, this threat is countered sufficiently.

- **T.ACCESS-SETTING (Unauthorized change of function setting condition related to security)**

This threat assumes the possibility of developing consequentially into the leakage of the user box files and secure print files by having been changed the specific function setting which relates to security.
O.CONFIG regulates that only the administrator is permitted to perform the setup of the enhanced security function that controls all setting function related to a series of security, and so the possibility of the threat is removed.
OE.FEED-BACK uses the application regulating that the feedback protected is returned for the entered passwords by the administrator's authentication, and OE.SESSION is also requested to logoff respectively after the operations of the administrator mode or service mode ends, so that O.CONFIG is supported sufficiently.
Accordingly, this threat is countered sufficiently.

4.3.4. Sufficiency of Organizational Security Policies

The organizational security policy is not applied.

5. Extended Components Definition

5.1. Extended Function Component

In this ST, three extended function components are defined. The necessity of each security function requirement and the reason of the labeling definition are described.

- **FAD_RIP.1**

  This is the security function requirement for the protection of the remaining information of user data and TSF data.

  - Necessity of extension

    The regulation for the protection of the TSF data remaining information is necessary. But the security function requirement to explain the protection of the remaining information exists only in FDP_RIP.1 for the user data. There is no security function requirement to satisfy this requirement.

  - Reason for applied class (FAD)

    There is no requirement to explain both of the user data and the TSF data with no distinction. Therefore, new class was defined.

  - Reason for applied family (RIP)

    As this is the extension up to the TSF data by using the content explained by the relevant family of FDP class, the same label of this family was applied.

- **FIA_EID.1**

  This is the security function requirement for regulating the conditions of accessing to the external entity from TOE.

  - Necessity of extension

    This is not approved the act accessed TOE from an external entity, but it is approval to the act that TOE itself moves to an external entity. There is no security function requirement to satisfy this requirement.

  - Reason for applied class (FIA)

    Since this regulates to identify the external entity, FIA class which defines each security function requirement of identification authentication is appropriate.

  - Reason for applied family (EID)

    This requirement content does not correspond to the one that the content was extended to an exsisting family. So, new family is defined.

- **FIT_CAP.1**

  This is the security function requirement for regulating the necessary ability for TOE to use effectively the security function of the external entity, IT environment.

  - Necessity of extension

    In case of TOE using the external security functions, the external security function to be surely secure is important, but TOE ability to provide is very important in order to use correctly the external security function. However, there is no concept as this requirement in the security function requirements.

  - Reason for applied class (FIT)

    There is no such concept in CC part 2. Therefore, new class was defined.

- Reason for applied family (CAP.1)

As similar to class, there is no such concept in CC part 2. Therefore, new family was defined.

5.1.1. FAD_RIP.1 Definition

- **Class name**

FAD: Protection of all data

Meaning of abbreviation: FAD (Functionaly requirement for All Data protection)

- **Class behavior**

This class contains a family specifying the requirement related with the protection of the user data and the TSF data with no distinction. One family exists here.

- Remaining Information Protection of All Data (FAD_RIP);

- **Family behavior**

This family corresponds to the necessity never to access the deleted information and newly created object and TSF data do not include the information that should not set as accessible. This family requires the protection for the information that was deleted or released logically but has a possibility to exist still in TOE.

- **Component leveling**

FAD_RIP: Remaining Information Protection of All Data	1

FAD_RIP.1: "Remaining Information Protection of All Data after the explicit deletion operation" requires of TSF to assure that the subset of the defined object controlled by TSF cannot utilize every remaining information of every resource under the allocation of resource or the release of it.

Audit : FAD_RIP.1
The use of the user identification information with the explicit deletion operation
Management : FAD_RIP.1
No expected management activity

FAD_RIP.1	**Remaining Information Protection of All Data after the explicit deletion operation**
FAD_RIP.1.1	
TSF shall ensure that the content of the information allocated to source before shall not be available after the explicit deletion operation against the object and TSF data.: [assignment: object list and TSF data list]	
Hierarchical to	: No other components
Dependencies	: No dependencies

5.1.2. FIA_EID.1 Definition

- **Family behavior**

This family corresponds to the necessity to ensure that IT environment entity is not replaced

illegally, when IT environment entity outside TOE provides the security function.
This family requires verifying the validity of IT environment entity.

- **Component leveling**

FIA_EID: External entity identification	1

Meaning of abbreviation: EID (External entity IDentification)

FIA_EID.1: "IT environment entity identification becoming an access object of TOE" requires the success of validity verification for IT environment entity before the action is involved in IT environment entity.

Audit : FIA_EID.1	
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.	
a) Minimal	Unsuccessful use of IT environment entity identification mechanism including offered IT environment entity identification information
b) Basic	Use all of IT environment entity identification mechanism including offered IT environment entity identification information
Management : FIA_EID.1	
The following actions could be considered for the management functions in FMT. a) management of IT environment entiry identification information	

FIA_EID.1	**Identification of IT environment becoming an access object from TOE**
FIA_EID.1.1	
TSF shall demand to succeed in the IT environment entity's identification before the action is taken to IT environment entity by TOE.	
FIA_EID.1.2	
TSF shall stop the start of the action to IT environment entity by TOE if the IT environment entity's identification is failed.	
Hierarchical to	: No other components
Dependencies	: No dependencies

5.1.3. FIT_CAP.1 Definition

- **Class name**

FIT: Support for IT environment entity
Meaning of abbreviation: FIT (Functional requirement for IT environment support)

- **Class behavior**

This class contains a family specifying the requirement related with the use of the security service provided by IT environment entity. One family exists here.

- Use of IT environment entity (FIT_CAP);

- **Family behavior**

This family corresponds to the capability definition for TOE at the use of security function of

IT environment entity.

- **Component leveling**

FIT_CAP: Capability of using IT environment entity	1

Meaning of abbreviation: CAP (**CAP**ability of using it environment)

FIT_CAP.1: "Capability of using security service of IT environment entity" corresponds to the substantiation of capability needed to use the security function correctly provided by IT environment entity.

Audit : FIT_CAP.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST. a) Minimal Failure of operation for IT environment entity b) Basic Use all operation of IT environment entity (success, failure)
Management : FIT_CAP.1
The following actions could be considered for the management functions in FMT. There is no management activity expected.

FIT_CAP.1	**Capability of using security service of IT environment entity**
FIT_CAP.1.1	
TSF shall provide the necessary capability to use the service for [assignment: *security service provided by IT environment entity*]. : [assignment: *necessary capability list for the operation of security service*]	
Hierarchical to	: No other components
Dependencies	: No dependencies

6. IT Security Requirements

In this chapter, the TOE security requirements are described.

<Definition of Label >

The security function requirements required for the TOE are described. Those regulated in CC Part 2 will be directly used for the functional requirements components, and the same labels will be used as well. The new additional requirement which is not described in CC part 2 is newly established and identified with the label that doesn't compete with CC part 2.

< Method of specifying security function requirement "Operation" >

In the following description, when items are indicated in “italic” and “bold,” it means that they are assigned or selected. When items are indicated in “italic” and “bold” with parenthesis right after the underlined original sentences, it means that the underlined sentences are refined. A number in the parentheses after a label means that the functional requirement is used repeatedly.

<Method of clear indication of dependency >

The label in the parentheses "( )" in the dependent section indicates a label for the security functional requirements used in this ST. When it is a dependency that is not required to be used in this ST, it is described as "N/A" in the same parentheses.

6.1. TOE Security Requirements

6.1.1. TOE Security Function Requirements

6.1.1.1. Cryptographic Support

FCS_CKM.1	**Cryptographic key generation**
FCS_CKM.1.1	
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].	
[assignment: *list of standards*] : ***KonicaMinolta Encryption specification standard***	
[assignment: *cryptographic key generation algorithm*] : ***KonicaMinolta HDD Encryption Key Generation Algorithm***	
[assignment: *cryptographic key sizes*] : ***128 bits***	
Hierarchical to : No other components Dependencies : FCS_CKM.2 or FCS_COP.1 (N/A), FCS_CKM.4 (N/A)	

6.1.1.2. User data protection

FDP_ACC.1[1]	**Subset access control**
FDP_ACC.1.1[1]	
The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].	
[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*] : ***Listed in "Table 2 User Box Access Control Operational*** List*"*	
[assignment: *access control SFP*] : ***User Box access control***	
Hierarchical to : No other components Dependencies : FDP_ACF.1 (FDP_ACF.1[1])	

Table 2 User Box Access Control Operational List

Subject	Object	Operational list
A task to act for a user	***User Box File***	• ***Download*** • ***Print*** • ***Transmission*** ***(E-mail transmission, FTP transmission, SMB transmission)***

FDP_ACC.1[2]	**Subset access control**
FDP_ACC.1.1[2]	
The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].	
[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*] : ***Listed in "Table 3 secure print file access control Operational List"***	
[assignment: *access control SFP*] : ***Secure Print file access control***	
Hierarchical to :	No other components
Dependencies :	FDP_ACF.1(FDP_ACF.1[2])

Table 3 Secure Print File Access Control Operational List

Subject	Object	Operational list
A task to act for a user	***Secure print file***	***Print***

FDP_ACC.1[3]	**Subset access control**
FDP_ACC.1.1[3]	
The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].	
[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*] : ***Listed in "Table 4 Administrator mode access control operational list"***	
[assignment: *access control SFP*] : ***Administrator mode access control***	
Hierarchical to :	No other components
Dependencies :	FDP_ACF.1(FDP_ACF.1[3])

Table 4 Administrator Mode Access Control Operational List

Subject	Object	Operational list
A task to act for a user	***- SMTP Server Group Object*** ***- DNS Server Group Object*** ***- MFP Address Group Object*** ***-Transmission Address Data Object***	***Settings***

FDP_ACF.1[1]	**Security attribute based access control**
FDP_ACF.1.1[1]	
The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].	
[assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*] : ***<Subject >*** ***<Subject attributes >*** ***- A task to act for a user*** → ***- User Box Attribute (User Box ID)*** --- ***<Object >*** ***<Object attributes >*** ***- User Box File*** → ***- User Box attributes (User Box ID)***	
[assignment: *access control SFP*] :	

User Box access control
FDP_ACF.1.2[1]
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*] : ***A task to act for a user who is related to the user box attributes (User Box ID) is permitted to download, print and transmit (E-mail transmission, FTP transmission, SMB transmission) to the user box file with the user box attribute corresponding to the user box attribute of the subject attribute.***
FDP_ACF.1.3[1]
The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects].
[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] : ***None***
FDP_ACF.1.4[1]
The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].
[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] : ***None***
Hierarchical to : No other components Dependencies : FDP_ACC.1(FDP_ACC.1[1]) , FMT_MSA.3(N/A)

FDP_ACF.1[2] **Security attribute based access control**
FDP_ACF.1.1[2]
The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].
[assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*] : ***<Subject >*** ***<Subject attributes >*** ***- a task to act for auser*** → ***- File attribute(secure print internal control ID)*** --- ***<Object >*** ***<Object attributes >*** ***- secure print file*** → ***- File attribute(secure print internal control ID)***
[assignment: *access control SFP*] : ***secure print file access control***
FDP_ACF.1.2[2]
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*] : ***A task to act for a user who has file attributes (secure print internal control ID) is permitted to print the secure print file that has a matching file attribute (secure print internal control ID) with the file attribute (secure print internal control ID).***
FDP_ACF.1.3[2]
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].
[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] : ***None***
FDP_ACF.1.4[2]
The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].
[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] :

None		
Hierarchical to	:	No other components
Dependencies	:	FDP_ACC.1(FDP_ACC.1[2]) , FMT_MSA.3(FMT_MSA.3)

FDP_ACF.1[3]	**Security attribute based access control**

FDP_ACF.1.1[3]

The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

[assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*] :

<Subject > ***<Subject attributes >***

- task to act for a user → ***- Administrator attributes***

<Object >

- SMTP server group object

- DNS server group object

- MFP address group object[6]

- Transmission address data file object

****Object attributes does not exist.***

[assignment: *access control SFP*] :

Administrator mode access control

FDP_ACF.1.2[3]

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*] :

A task to act for a user who had administrator attribute is permitted the setting operation of the SMPT server group object, DNS server group object, MFP address group object, and transmission data file object.

FDP_ACF.1.3[3]

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] :

None

FDP_ACF.1.4[3]

The TSF shall explicitly deny access of subjects to objects based on the [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] :

None

Hierarchical to	:	No other components
Dependencies	:	FDP_ACC.1 (FDP_ACC.1[3]), FMT_MSA.3 (N/A)

FDP_RIP.1	**Subset residual information protection**

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*].

[6] MFP address group object is the series of data concerning MFP address such as IP address, Appletalk printer name etc.

[selection: *allocation of the resource to, deallocation of the resource from*] : ***deallocation of the resource from***
[assignment: *list of objects*] : ***- All user box file*** ***- Swap data file*** ***- Overlay image file*** ***- HDD accumulation image file***
Hierarchical to : No other components
Dependencies : No dependencies

6.1.1.3. Identification and Authentication

FIA_AFL.1[1] **Authentication failure handling**
FIA_AFL.1.1[1]
The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].
[assignment: *list of authentication events*] : ***- Authentication for accessing the service mode*** ***- Re-authentication for changing the service code***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] ***[assignment: positive integer number] : 3***
FIA_AFL.1.2[1]
When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].
[selection: *met, surpassed*] : ***Met***
[assignment: *list of actions*] : ***<An action when it is detected >*** ***- Log off from the authentication status of the service mode if it is, and lock the authentication function which uses the service code*** ***- If it's not under the authentication status, lock the authentication function which uses the service code*** ***<Operation for recovering the normal condition >*** ***Perform the boot process of the TOE.***
Hierarchical to : No other components
Dependencies : FIA_UAU.1 (FIA_UAU.2[1])

FIA_AFL.1[2] **Authentication failure handling**
FIA_AFL.1.1[2]
The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].
[assignment: *list of authentication events*] : ***- Authentication for accessing administrator mode*** ***- Re-authentication for changing the administrator password***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] ***[assignment: positive integer number] : 3***
FIA_AFL.1.2[2]
When the defined number of unsuccessful authentication attempts has been [selection: *met,*

surpassed], the TSF shall [assignment: *list of actions*].
[selection: *met, surpassed*] : ***Met***
[assignment: *list of actions*] : ***<An action when it is detected > - Log off from the authentication status of the administrator mode if it is, and lock the authentication function which uses the administrator password. - If it's not under the authentication status, lock the authentication function which uses the administrator password. <Operation for recovering the normal condition > Perform the boot process of the TOE.***
Hierarchical to : No other components
Dependencies : FIA_UAU.1(FIA_UAU.2[2])

FIA_AFL.1[3]	**Authentication failure handling**

FIA_AFL.1.1[3]
The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].
[assignment: *list of authentication events*] : ***Authentication for accessing the secure print file.***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] ***[assignment: positive integer number] : 3***
FIA_AFL.1.2[3]
When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].
[selection: *met, surpassed*] : ***Met***
[assignment: *list of actions*] : ***<An action when it is detected > Refuse the access to the secure print file, and lock the authentication function to the secure print file <Operation for recovering the normal condition > Perform Lock release function offered in administrator mode.***
Hierarchical to : No other components
Dependencies : FIA_UAU.1(FIA_UAU.2[3])

FIA_AFL.1[4]	**Authentication failure handling**

FIA_AFL.1.1[4]
The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].
[assignment: *list of authentication events*] : ***Authentication for accessing the user box.***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] ***[assignment: positive integer number] : 3***
FIA_AFL.1.2[4]
When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].
[selection: *met, surpassed*] : ***Met***
[assignment: *list of actions*] :

<An action when it is detected > ***Refuse the access to the user box and the user box file in it, and lock the authentication function to the appropriate user box*** ***<Operation for recovering the normal condition >*** ***- Perform the Lock release function offered in administrator mode.*** ***- Perform the boot process of the TOE.***
Hierarchical to : No other components
Dependencies : FIA_UAU.1(FIA_UAU.2[4])

FIA_ATD.1	**User attribute definition**
FIA_ATD.1.1	
The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].	
[assignment: *list of security attributes*] : ***- User Box attributes (User Box ID)*** ***- File attributes (secure print internal control ID)*** ***- Administrator attributes***	
Hierarchical to : No other components	
Dependencies : No dependencies	

FIA_SOS.1[1]	**Verification of secrets**
FIA_SOS.1.1[1]	
The TSF shall provide a mechanism to verify that secrets ***(Administrator Password)*** meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*] : ***- Number of digits: 8- digits*** ***- Character type: possible to choose from 10 or more characters*** ***- Rule: Do not compose by only the same type of characters.***	
Hierarchical to : No other components	
Dependencies : No dependencies	

FIA_SOS.1[2]	**Verification of secrets**
FIA_SOS.1.1[2]	
The TSF shall provide a mechanism to verify that secrets ***(Secure Print Password, User Box Password)*** meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*] : ***- Number of digits: 8- digits*** ***- Character type: possible to choose from 92 or more characters*** ***- Rule: Do not compose by only the same type of characters.***	
Hierarchical to : No other components	
Dependencies : No dependencies	

FIA_SOS.1[3]	**Verification of secrets**
FIA_SOS.1.1[3]	
The TSF shall provide a mechanism to verify that secrets ***(HDD Lock Password, Encryption key passphrase)*** meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*] :	

- Number of digits: 20- digits ***- Character type: possible to choose from 82 or more characters*** ***- Rule: Do not compose by only same type of characters.***
Hierarchical to : No other components
Dependencies : No dependencies

FIA_SOS.1[4]	**Verification of secrets**
FIA_SOS.1.1[4]	
The TSF shall provide a mechanism to verify that secrets ***(Service Code)*** meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*] : ***- Number of digits: 8- digits*** ***- Character type: possible to choose from 12 or more characeters*** ***- Rule: Do not compose by only same type of characters.***	
Hierarchical to : No other components	
Dependencies : No dependencies	

FIA_UAU.2[1]	**User authentication before any action**
FIA_UAU.2.1[1]	
The TSF shall require each user ***(Service Engineer)*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***(Service Engineer)***.	
Hierarchical to : FIA_UAU.1	
Dependencies : FIA_UID.1 (FIA_UID.2[1])	

FIA_UAU.2[2]	**User authentication before any action**
FIA_UAU.2.1[2]	
The TSF shall require each user ***(Administrator)*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***(Administrator)***.	
Hierarchical to : FIA_UAU.1	
Dependencies : FIA_UID.1(FIA_UID.2[2])	

FIA_UAU.2[3]	**User authentication before any action**
FIA_UAU.2.1[3]	
The TSF shall require each user ***(User who is permitted to use secure print file)*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***(User who is permitted to use secure print file)***.	
Hierarchical to : FIA_UAU.1	
Dependencies : FIA_UID.1(FIA_UID.2[3])	

FIA_UAU.2[4]	**User authentication before any action**
FIA_UAU.2.1[4]	
The TSF shall require each user ***(User who is permitted to use user box)*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***(User who is permitted to use user box)***.	

Hierarchical to	:	FIA_UAU.1
Dependencies	:	FIA_UID.1(FIA_UID.2[4])

FIA_UAU.6	**Re-authenticating**

FIA_UAU.6.1

The TSF shall re-authenticate the use under the conditions [assignment: *list of conditions under which re-authentication is required*].

[assignment: *list of conditions under which re-authentication is required*]

- ***When the administrator modifies the administrator password***
- ***When the service engineer modifies the service code***
- ***When the administrator changes the setting of the HDD lock function***
- ***When the administrator changes the setting of the encryption function***

Hierarchical to	:	No other components
Dependencies	:	No dependencies

FIA_UAU.7	**Protected authentication feedback**

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*] :

Display "*" every character data input.

Hierarchical to	:	No other components
Dependencies	:	FIA_UAU.1(FIA_UAU.2[1] , FIA_UAU.2[2] , FIA_UAU.2[3], FIA_UAU.2[4])

FIA_UID.2[1]	**User identification before any action**

FIA_UID.2.1[1]

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

Hierarchical to	:	FIA_UID.1
Dependencies	:	No dependencies

FIA_UID.2[2]	**User identification before any action**

FIA_UID.2.1[2]

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

Hierarchical to	:	FIA_UID.1
Dependencies	:	No dependencies

FIA_UID.2[3]	**User identification before any action**

FIA_UID.2.1[3]

The TSF shall require each user ***(User who is permitted to use secure print file)*** to identify itself before allowing any other TSF-mediated actions on behalf of that user***(User who is permitted to use secure print file)*** **.**

Hierarchical to	:	FIA_UID.1

Dependencies	:	No dependencies

FIA_UID.2[4]	**User identification before any action**

FIA_UID.2.1[4]
The TSF shall require each user ***(User who is permitted to use the user box)*** to identify itself before allowing any other TSF-mediated actions on behalf of that user***(User who is permitted to use the user box)*** **.**
Hierarchical to : FIA_UID.1
Dependencies : No dependencies

FIA_USB.1	**User-subject binding**

FIA_USB.1.1
The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*]:
[assignment: list of user security attributes]: • ***User box attributes (user box ID)*** • ***File attributes (secure print internal control ID)*** • ***Administrator attribute***
FIA_USB.1.2
The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].
[assignment: *rules for the initial association of attributes*]: • ***As for the user box attribute, the user box ID of the concerned user box associates to the task acting on the behalf of users when authenticated with the access to the user box.*** • ***As for the file attribute, the secure print internal control ID of the concerned secure print file associates to the task acting on the behalf of users when authenticated with the access to the secure print file.*** ***As for the administrator attribute, the administrator's attributes associate to the task acting on the behalf of users when authenticated with the access to the administrator***
FIA_USB.1.3
The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].
[assignment: *rules for the changing of attributes*]. ***None***
Hierarchical to : No other components
Dependencies : FIA_ATD.1

6.1.1.4. Security Management

FMT_MOF.1	**Management of security functions behaviour**

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*] : ***Enhanced Security Setting***
[selection: *determine the behaviour of, disable, enable, modify the behaviour of*] : ***disable***
[assignment: *the authorised identified roles*] : ***Administrator***

Hierarchical to	:	No other components
Dependencies	:	FMT_SMF.1(FMT_SMF.1) , FMT_SMR.1(FMT_SMR.1[2])

FMT_MSA.1	**Management of security attributes**

FMT_MSA.1.1

The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete*, [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].

[assignment: *list of security attributes*] :
User box ID of the concerned user box

[selection: *change_default, query, modify, delete*, [assignment: *other operations*]] :
Modify

[assignment: *the authorized identified roles*] :
- User who is permitted to use that user box
- Administrator

Hierarchical to	:	No other components
Dependencies	:	FDP_ACC.1 or FDP_IFC.1 (FDP_ACC.1[1]) , FMT_SMF.1 (FMT_SMF.1) , FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[3])

FMT_MSA.3	**Static attribute initialisation**

FMT_MSA.3.1

The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes ***(secure print internal control ID)*** that are used to enforce the SFP.

[selection, choose one of: *restrictive, permissive, [assignment: other property]*] :
[assignment: other property]: Identified uniquely

[assignment: *access control SFP, information flow control SFP*] :
Secure print file access control

FMT_MSA.3.2

The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorised identified roles*] :
None

Hierarchical to	:	No other components
Dependencies	:	FMT_MSA.1(N/A) , FMT_SMR.1(N/A)

FMT_MTD.1[1]	**Management of TSF data**

FMT_MTD.1.1[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 authorised identified roles*].

[assignment: *list of TSF data*] :
"User Box password" of the concerned user box

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

[assignment: *the authorised identified roles*] :
- User who is permitted to use that user box
- Administrator

Hierarchical to	:	No other components
Dependencies	:	FMT_SMF.1(FMT_SMF.1), FMT_SMR.1(FMT_SMR.1[2], FMT_SMR.1[3])

FMT_MTD.1[2]	**Management of TSF data**
FMT_MTD.1.1[2]	
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 authorised identified roles*].	
[assignment: *list of TSF data*] : • ***Administrator password*** • ***Encryption key passphrase*** • ***HDD lock password***	
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***Modify***	
[assignment: *the authorised identified roles*] : ***Administrator***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1(FMT_SMF.1), FMT_SMR.1(FMT_SMR.1[2])

FMT_MTD.1[3]	**Management of TSF data**
FMT_MTD.1.1[3]	
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 authorised identified roles*].	
[assignment: *list of TSF data*] : ***Administrator password***	
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***Query, [assignment: other operations] : initialization***	
[assignment: *the authorised identified roles*] : ***Service engineer***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1(FMT_SMF.1), FMT_SMR.1(FMT_SMR.1[1])

FMT_MTD.1[4]	**Management of TSF data**
FMT_MTD.1.1[4]	
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 authorised identified roles*].	
[assignment: *list of TSF data*] : ***Service code***	
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***modify***	
[assignment: *the authorised identified roles*] : ***Service engineer***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1(FMT_SMF.1) , FMT_SMR.1(FMT_SMR.1[1])

FMT_MTD.1[5]	**Management of TSF data**
FMT_MTD.1.1[5]	
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 authorised identified roles*].
[assignment: *list of TSF data*] : • ***Secure print password*** • ***User box password***
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] : ***[assignment: other operations]: Resigtration***
[assignment: *the authorised identified roles*] : ***User***
Hierarchical to : No other components
Dependencies : FMT_SMF.1(FMT_SMF.1) , FMT_SMR.1(N/A)

FMT_SMF.1 Specification of Management Functions
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*] : • ***Stop function of enhanced security function by administrator*** • ***Deletion function of detected value of unauthorized access to secure print by administrator*** • ***Deletion function of detected value of unauthorized access to user box by administrator*** • ***Modification function of administrator password by administrator*** • ***Modification function of user box password by administrator*** • ***Modification function of user box ID by administrator*** • ***Modification function of HDD lock password by administrator*** • ***Modification function of encryption key passphrase by administrator*** • ***Operation setting function of Function to use encryption function realized by encryption board by administrator*** • ***Modification function of service code by service engineer*** • ***Inquiry function of administrator password by service engineer*** • ***Initialization function of administrator password by service engineer*** • ***Registration function of user box password by user*** • ***Registration function of user box ID by user*** • ***Registration function of user box by user*** • ***Modification function of user box password of the concerned user box by user who is permitted the use of user boxes*** • ***Modification function of user box ID of the concerned user box by user who is permitted the use of user boxes***
Hierarchical to : No other components
Dependencies : No dependencies

FMT_SMR.1[1] Security roles
FMT_SMR.1.1[1]
The TSF shall maintain the roles [assignment: *the authorised identified roles*].
[assignment: *the authorised identified roles*] : ***Service engineer***
FMT_SMR.1.2[1]
The TSF shall be able to associate users with roles.
Hierarchical to : No other components
Dependencies : FIA_UID.1 (FIA_UID.2[1])

FMT_SMR.1[2]	**Security roles**
FMT_SMR.1.1[2]	
The TSF shall maintain the roles [assignment: *the authorised identified roles*].	
[assignment: *the authorised identified roles*] : ***Administrator***	
FMT_SMR.1.2[2]	
The TSF shall be able to associate users with roles.	
Hierarchical to : No other components	
Dependencies : FIA_UID.1(FIA_UID.2[2])	

FMT_SMR.1[3]	**Security roles**
FMT_SMR.1.1[3]	
The TSF shall maintain the roles [assignment: *the authorised identified roles*].	
[assignment: *the authorised identified roles*] : ***User who is permitted to use secure print files***	
FMT_SMR.1.2[3]	
The TSF shall be able to associate users with roles.	
Hierarchical to : No other components	
Dependencies : FIA_UID.1(FIA_UID.2[3])	

FMT_SMR.1[4]	**Security roles**
FMT_SMR.1.1[4]	
The TSF shall maintain the roles [assignment: *the authorised identified roles*].	
[assignment: *the authorised identified roles*] : ***User who is permitted to use the user box***	
FMT_SMR.1.2[4]	
The TSF shall be able to associate users with roles.	
Hierarchical to : No other components	
Dependencies : FIA_UID.1(FIA_UID.2[4])	

6.1.1.5. Extension: Remaining All Information Protection

FAD_RIP.1	**Protection of all remaining information after explicit deletion operation**
FAD_RIP.1.1	
TSF shall guarantee not to be able to use the content of any information before having been assigned to the resource on the explicit deleting operation to the following objects and the TSF data: [assignment: *list of object and list of TSF data*].	
[assignment : *List of object and list of TSF data*] : ***<Objects>*** ***- Secure rpitn file*** ***- All user box files*** ***- Overlay image file*** ***- HDD remaining image file*** ***<TSF data>*** ***- HDD lock password*** ***- Administrator password*** ***- User Box password***	
Hierarchical to : No other components	

Dependencies	:	No dependencies

6.1.1.6. Extension: Approval of access destination

FIA_EID.1	**Identification of IT environment entity becoming an access object from TOE**
FIA_EID.1.1	
TSF shall demand to succeed in the IT environment entity's (***HDD***) identification before the action is taken to IT environment entity's (***HDD***) by TOE.	
FIA_EID.1.2	
TSF shall stop the start of the action to IT environment entity (***HDD***) by TOE if the IT environment entity's (***HDD***) identification is failed.	
Hierarchical to	: No other components
Dependencies	: No dependencies

6.1.1.7. Extension: Capability of Using IT Environment Entity

FIT_CAP.1[1]	**Capability of using security service of IT environment entity**
FIT_CAP.1.1[1]	
TSF shall provide the necessary capability to use the service for [assignment: *security service provided by IT environment entity*]. : [assignment: *necessary capability list for the operation of security service*]	
[assignment: *security service provided by IT environment entity*] : ***Encryption function achieved by encryption board***	
[assignment: *necessary capability list for the operation of security service*] : ***Support function of the image files processing by encryption function***	
Hierarchical to	: No other components
Dependencies	: No dependencies

FIT_CAP.1[2]	**Capability of using security service of IT environment entity**
FIT_CAP.1.1[2]	
TSF shall provide the necessary capability to use the service for [assignment: *security service provided by IT environment entity*]. : [assignment: *necessary capability list for the operation of security service*]	
[assignment: *security service provided by IT environment entity*] : ***HDD lock function achieved by HDD***	
[assignment: *necessary capability list for the operation of security service*] : • ***Support function of HDD lock password changing*** • ***Support function of HDD lock function releasing***	
Hierarchical to	: No other components
Dependencies	: No dependencies

6.1.2. TOE Security Assurance Requirements

The TOE is a commercial office product that is used in a general office environment, and therefore a TOE security assurance requirement that is required for EAL3 conformance, which is a sufficient level as an assurance for commercial office products, is applied. The following table summarizes the applied TOE security assurance requirements.

Table 5 TOE Security Assurance Requirements

TOE Security Assurance Requirements		Component
Class ADV: Development	Security architecture description	ADV_ARC.1
	Functional specification with complete summary	ADV_FSP.3
	Architectural design	ADV_TDS.2
Class AGD: Guidance documents	Operational user guidance	AGD_OPE.1
	Preparative procedures	AGD_PRE.1
Class ALC: Life Cycle Support	Authorisation controls	ALC_CMC.3
	Implementation representation CM coverage	ALC_CMS.3
	Delivery procedures	ALC_DEL1
	Identification of security measures	ALC_DVS.1
	Developer defined life-cycle model	ALC_LCD.1
Class ASE: Security Target Evaluation	Conformance claims	ASE_CCL.1
	Extended components definition	ASE_ECD.1
	ST introduction	ASE_INT.1
	Security objectives	ASE_OBJ.2
	Derived security requirements	ASE_REQ.2
	Security problem definition	ASE_SPD.1
	TOE summary specification	ASE_TSS.1
Class ATE: Tests	Analysis of coverage	ATE_COV.2
	Testing: basic design	ATE_DPT.1
	Functional testing	ATE_FUN.1
	Independent testing - sample	ATE_IND.2
Class AVA: Vulnerability Assessment	Vulnerability analysis	AVA_VLA.1

6.2. IT Security Requirements Rationale

6.2.1. Rationale for IT Security Functional Requirements

6.2.1.1. Necessity

The correspondence between the security objectives and the IT security functional requirements are shown in the following table. It shows that the IT security functional requirements correspond to at least one security objective.

Table 6 Conformity of IT Security Functional Requirements to Security Objectives

Security Objectives / Security Functional Requirements	O.BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.OVERWRITE-FILE	O.CRYPT-KEY	O.CHECK-HDD	O.CRYPTO-CAOABILITY	O.LOCK-HDD-CAPABILITY	* set.admin	* set.service
set.admin	X	X	X								
set.service	X	X	X								
FCS_CKM.1						X					
FDP_ACC.1[1]	X										
FDP_ACC.1[2]		X									
FDP_ACC.1[3]			X								
FDP_ACF.1[1]	X										
FDP_ACF.1[2]		X									
FDP_ACF.1[3]			X								
FDP_RIP.1					X						
FIA_AFL.1[1]											X
FIA_AFL.1[2]										X	
FIA_AFL.1[3]		X									
FIA_AFL.1[4]	X										
FIA_ATD.1	X	X	X								
FIA_SOS.1[1]										X	
FIA_SOS.1[2]	X	X									
FIA_SOS.1[3]			X								
FIA_SOS.1[4]											X
FIA_UAU.2[1]											X
FIA_UAU.2[2]										X	
FIA_UAU.2[3]		X									
FIA_UAU.2[4]	X										
FIA_UAU.6			X							X	X
FIA_UAU.7	X	X								X	X

Security Objectives / Security Functional Requirements	O.BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.OVERWRITE-FILE	O.CRYPT-KEY	O.CHECK-HDD	O.CRYPTO-CAOABILITY	O.LOCK-HDD-CAPABILITY	* set.admin	* set.service
FIA_UID.2[1]											X
FIA_UID.2[2]										X	
FIA_UID.2[3]		X									
FIA_UID.2[4]	X										
FIA_USB.1	X	X	X								
FMT_MOF.1			X								
FMT_MSA.1	X										
FMT_MSA.3		X									
FMT_MTD.1[1]	X										
FMT_MTD.1[2]										X	
FMT_MTD.1[3]										X	
FMT_MTD.1[4]											X
FMT_MTD.1[5]	X	X									
FMT_SMF.1	X	X	X							X	X
FMT_SMR.1[1]										X	X
FMT_SMR.1[2]	X		X							X	
FMT_SMR.1[3]		X									
FMT_SMR.1[4]	X										
FAD_RIP.1				X							
FIA_EID.1							X				
FIT_CAP.1[1]								X			
FIT_CAP.1[2]									X		

Note) ***set.admin*** and ***set.service*** indicates the set of the requirements. And the security objectives assumed to have the correspondence and presented by "**X**" also correspond to a series of requirement set associated by *set.admin and *set.service shown in columns.

6.2.1.2. Sufficiency

The IT security functional requirements for the security objectives are described as follows.

- **O.BOX (User Box Access Control)**

  This security objective limits the user box setting and the operation of the user box file in the user box only to the user who is permitted to use that user box, and needs various requirements that relate to the access control.

  <User box access control >

  It should be a user who is permitted to use the user box to operate the user box file in the user

box. FIA_UID.2[4] and FIA_UAU.2 [4] identifies and authenticates that a user is the authorised user to use the user box.
When the authentication failure reaches three times, FIA_AFL.1[4] locks the authentication function to the user box. This lock status is released by the TOE rebooting or the administrator's release operation.
When the user box ID is associated with the task of acting a use by FIA_ATD.1 and FIA_USB.1, the operation such as a download, print, and transmissions (E-mail transmission, FTP transmission, SMB transmission) is permitted to the user box file that has a corresponding object attribute to user box ID of the subject attribute.

<Management of user box >
FMT_MTD.1[1] permits the change in the user box password only to administrator and the authorized user to use the user box. FIA_SOS.1[2] verifies the quality of the user box password. FMT_MTD.1[5] permits the registration of user box password only to users.
Also, FMT_MSA.1 permits the change in the user box ID only to administrato and the user who is allowed to use that user box.

<Roles and controlling function for each management >
As the role of doing these managements, FMT_SMR.1[2] maintains an administrator and FMT_SMR.1[3] maintains a user permitted the use of the user box. FMT_SMF.1 specifies these management functions.

<Necessary requirement to keep the administrator secure >
→ refer to set.admin

<Necessary requirement to keep the service engineer secure >
→ refer to set.service

This security objective is satisfied by the completion of these multiple functional requirements.

- **O.SECURE-PRINT (Access control of secure print file)**

This security objective limits the print of secure print file only to the user who is permitted the use of the secure print file, and requires various requirements that relate to the access control.

<Access control of secure print file >
In order to print the secure print file, it should be a user who is permitted the use of the secure print file, and FIA_UID.2[3] and FIA_UAU.2[3] identify and authenticate if a user is a permitted user to use the secure print file.
FIA_AFL.1[3] locks the authentication function to the concerned user box when the authentication failure reaches three times. This lock status is released by the administrator's release operation.
FIA_UAU.7 returns "*" for each entered character as feedback protected and supports the authentication.
The internal control ID of the secure print is assoiciated with the task of acting use by FIA_ATD.1 and FIA_USB.1. And FDP_ACC.1[2] and FDP_ACF.1[2] allow the print operation to the secure print file that has corresponding object attribute to the secure print internal control ID of the subject attribute.

As for secure print internal control ID, FMT_MSA.3 gives the value uniquely identified when the secure print file is registered.

<Secure print password >
FMT_MTD.1[5] permits only to the user the registration of the secure print password used for the authentication FIA_SOS.1[2] verifies the quality of the secure print password.

<Roles and controlling function for each management >
As the role of doing these managements, FMT_SMR.1[3] maintains a user. FMT_SMF.1 specifies these management functions.

<Necessary requirement to keep the administrator secure >
→ refer to set.admin

<Necessary requirement to keep the service engineer secure >
→ refer to set.service

This security objective is satisfied by the completion of these multiple functional requirements.

- **O.CONFIG (Access limitation to management function)**

This security objective limits the setting related to the SMTP server, the setting related to the DNS server, the setting related to MFP address and the setting related to the enhanced security function to the administrator and service engineer, and needs various requirements to limit the access to a series of the setting function and the management function.

<Management of network setting >
When the administrator attribute is associated with the task of substituting the use, FDP_ACC.1[3] and FDP_ACF.1[3] permits the task of substituting the user to operate the settings for the SMTP server group object, DNS server group object, and MFP address group object.

<Operation limitation of Enhanced security function >
FMT_MOF.1 permits only the administrator to disable the setting for the enhanced security function.

<Management of HDD lock password, Encryption key passphrase >
When the administrator attribute is associated with the task of substituting the use by FIA_ATD.1 and FIA_USB.1, FDP_ACC.1[3] and FDP_ACF.1[3] permit the task of substituting the user to operate the setting of the HDD lock password object and encryption key passphrase object. FIA_SOS.1[3] verifies the quality of the HDD lock password and encryption key passphrase. In order to change the HDD lock password and encryption key passphrase, FIA_UAU.6 reauthenticates that a user is an administrator by collating with the registered HDD lock password and encryption key passphrase. When the authentication is succeeded, the change is permitted.

<Role and management function for each management >

FMT_SMR.1[2] maintains the role to do these management as a administrator. Also, FMT_SMF.1 specifies these management functions.

<Necessary requirement to keep the administrator secure >
→ refer to set.admin

<Necessary requirement to keep the service engineer secure >
→ refer to set.service

This security objective is satisfied by the completion of these multiple functional requirements.

- **O.OVERWRITE-ALL (Complete overwrite deletion)**

  This security objective regulates that it deletes all data areas of HDD and initializes the administrator password of NVRAM, and requires various requirements that relate to the deletion.
  FAD_RIP.1 guarantees that these objective information not to be able to use the content of any previous information by the deletion operation.

  This security objective is satisfied by the completion of these multiple functional requirements.

- **O.OVERWRITE-FILE (Overwrite Deletion of each file)**

  This security objective regulates that it deletes the image file written in HDD, which became unnecessary, and needs various requirements that relate to the deletion.
  FDP_RIP.1 guarantees these objective information (all user box files, swap data files, overlay image files, and HDD accumulation picture files) not to be able to use the content of any previous information when these are released from the allocation of the resource.

  This security objective is satisfied by the completion of these multiple functional requirements.

- **O.CRYPT-KEY (Encryption key generation)**

  This security objective regulates that the encryption key necessary to encrypt all the data written in HDD is generated, and needs various requirements that relate to the encryption key generation, when the encryption board is installed.
  Using Konica Minolta HDD encryption key generation mechanism according to the Konica Minolta encryption specification standard, FCS_CKM.1 generates an encryption key 128 bits long.
  This security objective is satisfied by the completion of this function requirement.

- **O.CHECK-HDD (Validity confirmation of HDD)**

  This security objective regulates that it verifies the validity of HDD in order to confirm the unauthorised HDD doesn't exist, and needs various requirements that relate to the verification of an external entity from TOE.
  FIA_EID.1 identifies HDD before the action from TOE to HDD, and cancels the scheduled action when the identification fails.
  This security objective is satisfied by the completion of this function requirement.

- **O.CRYPTO-CAPABILITY (Encryption of HDD)**

  This security objective regulates that TOE's support action for the data stored in HDD is encrypted by the encryption board that is the entity out of TOE, and needs various requirements that regulates the support of external entity action.

  Applying FIT_CAP.1[1], a support function to process image files through the encryption function implemented by the encryption board is achieved for that encryption function.

  This security objective is satisfied by the completion of this function requirement.

- **O.LOCK-HDD-CAPABILITY (Support action to use HDD lock function)**

  This security objective regulates that TOE's support action for it refuses the unauthorized access from MFP other than the one that is set by the HDD which is the entity out ot TOE, and needs various requirements that regulates the support of external entity action.

  Applying FIA_CAP.1[2], a support function to change HDD lock password and support function to release HDD lock function are achieved for the HDD lock function implemented by HDD.

  This security objective is satisfied by the completion of this function requirement.

- **OE.FEED-BACK (Feedback of password)**

  This security objective regulates that the application (used by client PC for accessing to MFP) that is the entity of a necessary IT environment for the TOE security maintenance provides the appropriate protected feedback for the entered user password, user box password and administrator password.

  Applying FIA_UAU.7, the application displays "*" for each character as feedback for entered character data.

  This security objective is satisfied by the completion of this function requirement.

The following is the compilation of set such as (1)the set of necessary requirement to keep administrator secure (set.admin), (2)the set of necessary requirement to keep service engineer secure (set.service).

- ***set.admin*** **(Set of necessary requirement to keep administrator secure)**

  <Identification and Authentication of an administrator >

  FIA_UID.2[2] and FIA_UAU.2[2] identifies and authenticates that the accessing user is a administrator.

  FIA_UAU.7 returns "*" for each character entered as feedback protected in the panel, and supports the authentication.

  FIA_AFL.1[2] locks all the authentication functions that use the administrator password when the failure authentication reaches three times. This lock is released by rebooting TOE such as turning the power OFF and ON.

  <Management of administrator's authentication information >

  FIA_SOS.1[1] verifies the quality of the administrator password. FMT_MTD.1[2] limits to the administrator the change in the administrator password. FIA_UAU.6 reauthenticates the administrator password when the administrator changes the administrator password. In this re-authentication, FIA_AFL.1[2] cancels the administrator authenticated state when the failure authentication reaches three times, and locks all the authentication functions to use

the administrator password. This lock state is released by rebooting TOE such as turning power OFF and ON.
Also, the inquiry of administrator's password and initialization are limited to the service engineer by FMT_MTD.1[3].

<Role and management function for each management >
FMT_SMR.1[1] have service engineer maintain the role to do these management, and FMT_SMR.1[2] have the administrator do the same. Additionally, FMT_SMF.1 specifies these management functions.

- ***set.service*** **(Set of necessary requirement to keep service engineer secure)**

<Identification and Authentication of a service engineer >
FIA_UID.2[1] and FIA_UAU.2[1] identifies and authenticates that the accessing user is a service engineer.
FIA_UAU.7 returns "*" each one character entered as the feedback protected, and supports the authentication.
FIA_AFL.1[1] locks all the authentication functions to use the service code when the failure authentication reaches three times. This lock is released by rebooting TOE such as turning the power OFF and ON.

<Management of service engineer's authentication information >
FIA_SOS.1[4] verifies the quality of the service code. FMT_MTD.1[4] restricts the chage in the service code to the service engineer. FIA_UAU.6 re-authenticates it. In this the re-authentication, FIA_AFL.1[1] releases the authentication status of the service engineer when the failure authentication reaches three times, and locks all the authentication functions to use the service code. This lock status is released by rebooting TOE such as turning power OFF and ON.

<Role and management function for each management >
FMT_SMR.1[1] maintains the role to do these management as a service engineer. FMT_SMF.1 specifies these management functions.

FPT_RVM.1 and FPT_SEP.1 are the security function requirements immediately not related to the security objective, though it is not included in the explanation of the sufficiency of the above-mentioned. But, it is shown in the mutual support described later to support the security function requirement that is included in the explanation of the sufficiency of the above-mentioned. Because these two security function requirements will relate to the security objective that corresponds to the security function requirement supported respectively by two security function requirements, the relation with the security objective is consequentially clear.

6.2.1.3. Dependencies of IT Security Functional Requirements

The dependencies of the IT security functional requirements components are shown in the following table. When a dependency regulated in CC Part 2 is not satisfied, the reason is provided in the section for the "Dependencies Relation in this ST."

Table 7 Dependencies of IT Security Functional Requirements Components

N/A : Not Applicable

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	<Reason for not applying FCS_CKM.2 or FCS_COP.1 > The cryptographic operation is performed in the IT environment by FIT_CAP.1[1]. TSF only uses this capability, and there is no necessity of the distribution and cryptographic operation. < Reason for not applying FCS_CKM.4 > The encryption key is regularly kept for the stored data. Moreover, an arbitrary access to the storage medium is difficult, and there is no necessity of the encryption key cancellation.
FDP_ACC.1[1]	FDP_ACF.1	FDP_ACF.1[1]
FDP_ACC.1[2]	FDP_ACF.1	FDP_ACF.1[2]
FDP_ACC.1[3]	FDP_ACF.1	FDP_ACF.1[3]
FDP_ACF.1[1]	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1[1] <Reason for not applying FMT_MSA.3 > The user box file, the generated object, has no security attribute to be managed other than user box ID as the identifier, therefore, there is no necessity to regulate the event to provide the default value with any characteristics as an object attribute. User box ID that is related to the user box file, is a value specified by the user operation and doesn't correspond to the event assumed with FMT_MSA.3. (Because the structure of limiting the selectable user box to the specified user at the time of generating the user box file is not necessary.)
FDP_ACF.1[2]	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1[2] FMT_MSA.3
FDP_ACF.1[3]	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1[3] <Reason for not applying FMT_MSA.3 > This requirement is not necessary to be applied because the object attribute doesn't exist.
FDP_RIP.1	None	N/A
FIA_AFL.1[1]	FIA_UAU.1	FIA_UAU.2[1]
FIA_AFL.1[2]	FIA_UAU.1	FIA_UAU.2[2]
FIA_AFL.1[3]	FIA_UAU.1	FIA_UAU.2[3]
FIA_AFL.1[4]	FIA_UAU.1	FIA_UAU.2[4]

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FIA_ATD.1	None	N/A
FIA_SOS.1[1]	None	N/A
FIA_SOS.1[2]	None	N/A
FIA_SOS.1[3]	None	N/A
FIA_SOS.1[4]	None	N/A
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1]
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2]
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3]
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[4]
FIA_UAU.6	None	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.2[4]
FIA_UID.2[1]	None	N/A
FIA_UID.2[2]	None	N/A
FIA_UID.2[3]	None	N/A
FIA_UID.2[4]	None	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMR_SMR.1	FDP_ACC.1[1] FMT_SMF.1 FMT_SMR.1[2], FMT_SMR.1[3]
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_SMR.1[3] <Reason for not applying FMT_MSA.1 > This is the internal control ID that is identified uniquely, and this does not require the management such as change or deletion, after this is assigned once.
FMT_MTD.1[1]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2], FMT_SMR.1[3]
FMT_MTD.1[2]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MTD.1[3]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]
FMT_MTD.1[4]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]
FMT_MTD.1[5]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 <Reason for not applying FMT_SMR.1> There is no restriction of users before registering passwords. Also, after the password is registered, the role is managed and maintained. There is no necessity of maintenance of the role on this step.
FMT_SMF.1	None	N/A
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2[1]
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[2]

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[3]
FTM_SMR.1[4]	FIA_UID.1	FIA_UID.2[4]
FAD_RIP.1	None	N/A
FIA_EID.1	None	N/A
FIT_CAP.1[1]	None	N/A
FIT_CAP.1[2]	None	N/A

6.2.2. Rationale for IT Security Assurance Requirements

This TOE is installed and used in an environment where adequate security is maintained in terms of the physical, personnel, and connectivity. Nonetheless, adequate effectiveness in the environment where the TOE is used must be assured. As a general commercial office product, the execution of tests based on function specifications and high level design, and analysis of the strength of function and a search for vulnerabilities are required. In addition, it is desirable that it has a development environment control, a configuration management for the TOE and a secure distribution procedure. And therefore the selection of EAL3, which provides an adequate assurance level is reasonable.

The assurance requirement dependency analysis is assumed to be appropriate because the package EAL has been selected, therefore details are not discussed.

7. TOE Summary Specification

The list of the TOE security function led from the TOE security function requirement is shown in Tables 8 below. The detailed specification is explained in the paragraphs described below.

Table 8 The list of the name and identifier of TOE Security function

No.	TOE Security function	Relationship with TOE Logical Scope
7.1	F.ADMIN (Administrator function)	Administrator function
7.2	F.SERVICE (Service mode function)	Service mode function
7.3	F.BOX (User box function)	User box function
7.4	F.PRINT (Secure print function)	Secure print function
7.5	F.OVERWRITE-FILE (Remaining information overwrite deletion function)	Other function
7.6	F.OVERWRITE-ALL (All area overwrite deletion function)	Administrator function
7.7	F.CRYPT (Encryption key generation function)	Other function
7.8	F.SUPPORT-CRYPTO (Encryption board operation support function)	Utilization of encryption board
7.9	F.VALIDATION-HDD (HDD validation function)	Utilization of HDD lock function
7.10	F.SUPPORT-HDD (HDD lock operation support function)	Utilization of HDD lock function
7.11	F.RESET (Authentication failure frequency reser function)	Other function

7.1. F.ADMIN(Administrator Function)

F.ADMIN is a series of security function that administrator operates, such as an administrator identification authentication function in an administrator mode accessing from a panel or through a network, and a security management function that includes a change of an administrator password and a lock cancellation of a locked user box. (Nevertheless, all functions are not feasible functions through both a panel and a network.)

7.1.1. Administrator Identification Authentication Function

It identifies and authenticates the accessing user as the administrator in response to the access request to the administrator mode.

- It provides the administrator password authentication mechanism authenticating by the administrator password that consists of the character shown in Table 9.
- Return "*" for each character as feedback for the entered administrator password by the access from the panel.
- Resets the number of authentication failure when succeeding in the authentication.
- Locks all the authentication functions to use the administrator password when detecting the authentication failure that becomes the third times at total in each authentication function by using the administrator password. (Refuse the access to the administrator mode)

- F.RESET works and the lock of authentication function is released.

  As described above, FIA_AFL.1[2], FIA_UAU.2[2], FIA_UAU.7 and FIA_UID.2[2] are realized.

Table 9 Characters and Number of Digits for Password

Objectives	Number of digits	Character
Service code	8	Selectable from 12 characters in total (Numeric, Some are symbols)
Administrator password	8	Selectable from 10 characters in total (Numeric)
User Box password Secure print password	8	Selectable from 92 characters in total (Alphabet, numeric, symbols (Some are not included))
HDD lock password Encryption key passphrase	20	Selectable from 82 characters in total (Alphabet, numeric, symbols (Some are not included))

7.1.2. Function Supported in Administrator Mode

When a user is identified and authenticated as an administrator by the administrator identification authentication function at the accessing request to the administrator mode, the administrator authority is associated with the task substituting the user. And the following operations and the use of the functions are permitted.

As described above, FIA_ATD.1 and FIA_USB.1 are realized.

7.1.2.1. Change of Administrator Password

When a user is re-authenticated as an administrator and the newly set password satisfies the quality, the password is changed.

- It provides the administrator password authentication mechanism that is authenticated by the administrator password which consists of the character shown in Table 9.
- Resets the number of authentication failure when succeeding in the re-authentication.
- Return "*" for each character as feedback for the entered administrator password in the re-authentication.
- When the authentication failure that becomes the third times at total in each authentication function by using the administrator password is detected, it logoffs the administrator mode accessing from the panel, and locks all the authentication functions to use the administrator password. (The access to the administrator mode is refused.)
- F.RESET works and the lock of authentication function is released.
- Verify the new administrator password if the following qualities are satisfied.
  - It is composed of the characters and by the number of digits, shown in the Table 9.
  - It shall not be composed of one kind of character.

As described above, FIA_AFL.1[2], FIA_SOS.1[1], FIA_UAU.6, FIA_UAU.7, FMT_MTD.1[2], FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.2.2. Change of User box password

The user box password other than the "Public" user box is changed. It verifies whether the user box password newly set have been satisfied the following qualities.

- It is composed of the characters and by the number of digits, shown in the Table 9
- It shall not be composed of one kind of character.

As described above, FIA_SOS.1[2], FMT_MTD.1[1], FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.2.3. Change of User box ID

The user box ID is changed to the unregistered one other than PUBLIC.
As described above, FMT_MSA.1, FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.2.4. Release of lock

Reset (clear all) the number of times of authentication failure for all secure prints and user boxes.

- If there is a secure print to which access is locked, the lock is released.

Reset (clear all) the number of times of authentication failure of all user boxes.

- If there is a user box to which access is locked, the lock is released.

As described above, FIA_AFL.1[3], FIA_AFL.1[4] and FMT_SMR.1[2] are realized.

7.1.2.5. Network Setup

A setup operation of the following setting data is performed.

- A series of setup data that relates to SMTP server. (IP addesess, Port Number, etc.)
- A series of setup data that relates to DNS server. (IP address, Port Number, etc.)
- A series of setup data that relates to MFP address (IP address, NetBIOS Name, AppleTalk Printer Name, etc.)

As described above, FDP_ACC.1[3], FDP_ACF.1[3] and FMT_SMR.1[2] are realized.

7.1.2.6. Operation Setup Function of HDD Lock Function

<Operation Setting ON>
When turing it ON from OFF, it verifies that the HDD lock password newly set satisfies the following qualities.

- It is composed of the characters and by the number of digits shown in Table 9.
- It shall not be composed of one kind of character.

<Operation Setting OFF>
Turning it OFF from ON. (It is only allowed when the encryption function is ON.)
When the user is re-authenticated as the administrator by using the HDD lock password currently set, it turns OFF.

- It provides the HDD lock password verification mechanism that verified the HDD lock password that consists of the character shown in Table 9.
- Return, in verification, "*" for each character as feedback for the entered HDD lock

password.

<HDD Lock Password Change>

The HDD lock password is changed. When it is re-authenticated by the currently setup HDD lock password that the user is an administrator, and the newly setup password satisfies quality requirements, it is changed.

- It provides the HDD lock password verification mechanism that verified the HDD lock password that consists of the character shown in Table 9.
- Return, in verification, "*" for each character as feedback for the HDD lock password.
- Verify the HDD lock password newly set if the following qualities are satisfied.
  - It is composed of the characters and by the number of digits shown in Table 9.
  - It shall not be composed of one kind of character.

As described above, FIA_SOS.1[3], FIA_UAU.7, FIA_UAU.6, FMT_MTD.1[2], FMT_SMF.1, FMT_SMR.1[2] and FIT_CAP.1[2] are realized.

7.1.2.7. Operation Setup of Encryption Function

It is operatable only when the encryption board option is installed in MFP.

<Operation Setting ON>

When turing it ON from OFF, it verifies that the encryption key passphrase newly set satisfies the following qualities, and F.CRYPT is performed.

- It is composed of the characters and by the number of digits shown in Table9.
- It shall not be composed of one kind of character.

<Operation Setting OFF>

Turning it OFF from ON. (It is only allowed when the HDD lock function is ON.)

When the user is re-authenticated as the administrator by using the encryption key passphrase currently set, it turns OFF.

- It provides the encryption key passphrase verification mechanism that verified the encryption key passphrase that consists of the character shown in Table 9.
- Return, in verification, "*" for each character as feedback for the entered encryption key passphrase.

<Encryption Key Passphrase Change>

The encryption key passphrase is changed. When it is re-authenticated by the currently setup encryption key passphrase that the user is an administrator, and the newly setup encryption key passphrase satisfies quality requirements, it is changed, and F.CRYPT is performed.

- It provides the encryption key passphrase verification mechanism that verified the encryption key passphrase that consists of the character shown in Table 9.
- Return, in verification, "*" for each character as feedback for the encryption key passphrase.
- Verify the encryption key passphrase newly set if the following qualities are satisfied.
  - It is composed of the characters and by the number of digits shown in Table 9.
  - It shall not be composed of one kind of character.

As described above, FIA_SOS.1[3], FIA_UAU.7, FIA_UAU.6, FMT_MTD.1[2], FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.2.8. Function Related to Password Initialization Function

The function that relates to the initialization of the password that the administrator operates is as follows.

- All area overwrite deletion function
  The settings of the administrator password is initialized to the values at factory shipment by executing the overwrite deletion of all area

As described above, FMT_MTD.1[2] , FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.1.2.9. Operation Setup of Enhanced Security Function

The function that influences the setup of the Enhanced Security function that the administrator operates is as follows.

- Operational setup of Enhanced Security function
  Function to set valid or invalid of Enhanced Security function
- All area overwrite deletion function
  The setup data of enhanced security function are invalidated by executing the overwrite deletion of all area.

As described above, MFT_MOF.1[1], FMT_SMF.1 and FMT_SMR.1[2] are realized.

7.2. F.SERVICE (Service Mode Function)

F.SERVICE is a series of security function that the service engineer operates, such as the service engineer identification authentication function in service mode accessing from a panel, and a security management function that includes a change in the service code and the administrator password.

7.2.1. Service Engineer Identification Authentication Function

It is identified and authenticated the accessing user as the service engineer in response to the access request to the service mode from the panel.

- Provides the service code authentication mechanism that is authenticated by the service code that consists of the character shown in Table 9.
- Return "*" for each character as feedback for the entered service codes.
- Resets the number of the authentication failure when succeeding in the authentication.
- When the authentication failure that becomes the third times at total in each authentication function by using the service code is detected, it locks all the authentication functions to use the service code. (The access to the service mode is refused.)
- Lock of authentication function is released with F.RESET function operated.

As described above, FIA_AFL.1[1], FIA_UAU.2[1], FIA_UAU.7 and FIA_UID.2[1] are realized.

7.2.2. Function Supported in Service Mode

When a user is identified and authenticated as a service engineer by the service engineer identification authentication function at the access request to the service mode, the use of the

following functions is permitted.

(1) Change of the Service Code

When a user is re-authenticated as a service engineer and the new password satisfies the quality, it is changed.

- Provides the service code authentication mechanism that is re-authenticated by the service code that consists of the characters shown in Table 9.
- Resets the authentication failure frequency when succeeding in the re-authentication.
- Return "*" for each character as feedback for the entered service codes in the re-authentication.
- When the authentication failure that becomes the third times at total in each authentication function by using the service code is detected, it logoffs the service mode accessing from the panel, and locks all the authentication functions to use the service code. (The access to the service mode is refused.)
- The F.RESET function unlocks the authentication function.
- It verifies the service code newly set satisfies the following qualities.
  - It is composed of the characters and by the number of digits, shown in the Table 9.
  - It shall not be composed of one kind of character.

As described above, FIA_AFL.1[1], FIA_SOS.1[4], FIA_UAU.6, FIA_UAU.7, FMT_MTD.1[4], FMT_SMF.1 and FMT_SMR.1[1] are realized.

(2) Initialization of Administrator Password

Initialize the administrator password. It is initialized to the values at factory shipment.

As described above, FIA_SOS.1[1], FMT_MTD.1[3], FMT_SMF.1 and FMT_SMR.1[1] are realized.

7.3. F.BOX(User Box Function)

F.BOX is a security function that relates to the user box such as the user box access control function, which identifies and authenticates that a person is a permitted user to use the user box in the accessing to the user box from a client PC or a panel and controls the operation to the user box files.

7.3.1. Registration function of user box

The user box registration operation is provides by the user operation from a client PC. When user box ID (unregistered one) and user box password is specified appropriately, the specified user box is registered.

- Verify that a user box password satisfies the following conditions.
  - It is composed of the characters and by the number of digits shown in the Table 9.
  - It shall not be composed of one kind of character.

As described above, FIA_SOS.1[2], FMT_MTD.1[5] and FMT_SMF.1 are realized.

7.3.2. Identification authentication function in access to user box

For the access request for each user box, the user who accesses is authenticated that it is a

user permitted the use of a user box concerned respectively.

- Provides the user box password authentication mechanism that is authenticated by the user box password that consists of the character shown in Table 9.
- Return "*" for each character as feedback for the entered user box password.
- Resets the number of authentication failure when succeeding in the authentication.
- When the authentication failure is detected the third times at total for a user box concerned, it locks the authentication function to the user box.
- The lock of the authentication function executes the lock release function to the user box of F.ADMIN or operates F.RESET function and releases the lock of the user box.

(1) Access control to user box file in the user box from a panel

The task to act for the user is related to the "User Box ID" of the user box as a user box attribute. This task is permitted the user box file, which have a corresponding user box attribute to the user box attribute of the subject attribute, to do the printing, transmission (E-mail transmission, FTP transmission, SMB transmission) operation.

As described above, FDP_ACC.1[1], FDP_ACF.1[1], FIA_ATD.1 and FIA_USB.1 are realized.

The followings are the function that the user who is permitted the use of the user box is provided in the user box operation of the user box, and to execute it from the client PC , authenticaion is required for all.

- Provides the user box password authentication mechanism that is authenticated by the user box password that consists of the character shown in Table 9.
- Resets the number of authentication failure of a user box concerned when succeeding in the authentication.
- Return "*" for each character as feedback for the entered user box password.
- When the authentication failure is detected the third times at total in each authentication function to use the user box password, it logs off the user box identification authentication domain, and locks all the authentication functions to use the user box password.(The access of a user box concerned to the user box identification authentication domain is refused.)
- The lock of the authentication function executes the lock release function to the user box of F.ADMIN, or operates F.RESET function and releases the lock of the user box.

As descrived above, FIA_AFL.1[4], FIA_UAU.2[4], FIA_UAU.7, FIA_UID.2[4] and FMT_SMR.1[4] are realized.

(2) Access control to user box file in the user box from the client PC

The task to act for the user is related to the "User Box ID" of the user box as a user box attribute. This task is permitted the user box file, which have a corresponding user box attribute to the user box attribute of the subject attribute, to do the downloading.

As described above, FDP_ACC.1[1], FDP_ACF.1[1], FIA_ATD.1 and FIA_USB.1 are realized.

(3) Change of user box password from the client PC

The user box password of the user box is changed.

- Verify that the user box password newly set satisfies the following quality.
  - It is composed of the characters and by the number of digits shown in the Table 9.
  - It shall not be composed of one kind of character.

As described above, FIA_SOS.1[2], FMT_MTD.1[1], FMT_SMF.1 and FMT_SMR.1[4] are realized.

(4) Change of user box ID from the client PC

User box ID of the user box is changed to the unregistered one other than PUBLIC.

As described above, FMT_MSA.1, FMT_SMF.1 and FMT_SMR.1[4] are realized.

7.4. F.PRINT (Secure Print Function)

F.PRINT is a series of security function related to the secure print such as the access control function that allows the printing the secure print file after authenticating if a user is the authorized person to use the secure print file for the access to the secure print file from the panel.

7.4.1. Authentication Function by secure print password

It authenticates that the accessing user is a user to whom the use of the secure print file concerned is permitted, in response to the access request to each secure print file.

- Provides the secure print password authentication mechanism that is authenticated by the secure print password that consists of the character shown in Table 9.
- Return "*" for each character as feedback for the entered secure print password.
- When the authentication failure that becomes three times in total for the secure print file concerned is detected, the authentication function to the concerned secure print file is locked.
- The lock status is released by the lock release function to the secure print file of F.ADMIN executed.

As described above, FIA_AFL.1[3], FIA_UAU.2[3], FIA_UAU.7, FIA_UID.2[3] and FMT_SMR.1[3] are realized.

7.4.2. Access Control Function to Secure Print File

The secure print file access control operates when it is authenticated.

- The task to act for the user who is identified and authenticated has the secure print ID of the authenticated secure print file as the file attribute.
- This task is permitted the printing to the secure print file with a corresponding file attribute to the file attribute of this task.

As described above, FIA_ATD.1, FIA_USB.1, FDP_ACC.1[2], FDP_ACF.1[2] and FMT_SMR.1[3] are realized.

7.4.3. Registration Function of Secure Print File

(1) Registration of the secure print password

The registered secure print password is verified to meet the following requirements in a registration request of the secure print file.

- It is composed of the characters and by the number of digits shown in the Table 9.
- It shall not be composed of one kind of character.

(2) Giving of the secure print internal control ID

When the verification of the secure print password is completed in a registration request of

the secure print file, the secure print internal control ID uniquely identified is set to the concerned secure print file.

As described above, FIA_SOS.1[2], FMT_MTD.1[5] and FMT_MSA.3 are realized.

7.5. F.OVERWRITE-FILE (Remaining information overwrite deletion function)

F.OVERWRITE is not only the general deletion (deletion of the management area for the file access), but also the overwrite deletion function of the HDD data domain when deleting a file in the following cases.

<Event that remaining information overwrite deletion starts >

- Job completion of copy and print.
  - Overwrite deletion object: Swap data file
- Deletion by user operation.
  - Overwrite deletion object: All user box files, overlay image files, HDD accumulation image files
- Start of automatic deletion by time limit passage.
  - Overwrite deletion object: All user box files, swap data files(Only the swap data of the secure print file corresponds)
- When the power is turned on after the power was turned off while the job is running.
  - Overwrite deletion object : Swap data files

The deletion method is "0x00→0x00→0x00" and overwrite the object area.

As described above, FDP_RIP.1 is realized.

7.6. F.OVERWRITE-ALL (All area overwrite deletion function)

F.OVERWRITE-ALL executes the overwrite deletion in the data area of HDD, and initializes the settings such as passwords on NVRAM as well. The object for the deletion or initialization is as follows.

<Object for the deletion : HDD >

- All user box files
- Swap data file
- Overlay image file
- HDD accumulation image file
- User box password

<Object for the deletion : NVRAM[7] >

- Transmission address data file

<Object for the initialization : NVRAM >

- Administrator password

[7] Service code, HDD lock password and encryption key passphrase in NVRAM is also initialized, but these is no way to confirm the values after it is returned or discarded even if these TSF data does not deleted. And so, it is not contained in the indispensable objects for the deletion.

The deletion method for the data and the frequency written in HDD executes "0x00→0xFF→0x00→0xFF→0x00→0xFF→0xAA→ verification".

As described above, FAD_RIP.1 is realized.

7.7. F.CRYPT (Encryption Key Generation Function)

F.CRYPT generates an encryption key to encrypt all data written in HDD by using the SHA-1 algorithm that is specified as the satandard (FIPS 180-1) by National Institute of Standards and Technology: NIST.

When the encryption key passphrase is decided in the encryption functional operation setting to which the access is restricted in F.ADMIN, an encryption key 128 bits long is generated from the encryption key passphrase by applying the SHA-1 algorithm.

As described above, FCS_CKM.1 is realized.

7.8. F.SUPPORT-CRYPTO (Encryption Board Operation Support Function)

F.SUPPORT-CRYPTO is the function that operates the encryption function that utilizes encryption board from TOE.

For all data written in HDD, an encryption key generated by F.CRYPTO is set in the encryption board, and encryption is performed by the encryption board. Also, for the encrypted image files read out of the HDD, the encryption key generated by F.CRYPTO is set in encryption board in the same manner as above, and decryption is performed by the encryption board.

As described above, FIT_CAP.1[1] is realized.

7.9. F.VALIDATION-HDD (HDD Verification Function)

F.VALIDATION-HDD is the check function to permit reading and writing HDD only when it is verified and comfirmed that the illegal HDD is not set, when HDD lock password is set in HDD.

When HDD lock password is set in HDD, the status confirmation of HDD is performed for the HDD operation confirmation of the TOE activation. As the result of the status confirmation, if the HDD lock password is certainly set, the access to HDD is premitted, and if it is not, the access to HDD is denied since there is an illegal possibility.

As described above, FIA_EID.1 is realized.

7.10. F.SUPPORT-HDD (HDD Lock Operation Support Function)

F.SUPPORT-HDD is the function that operates the HDD lock function by HDD from TOE.

<Release process of HDD lock status>

When MFP is started, the release process for releasing the lock status by HDD lock function of HDD is performed.

- The release process request is executed to HDD by using HDD lock password stored in

NVRAM.

<Process based on the chage of HDD lock password>

The change process request of HDD lock password from F.ADMIN is performed.

- The change process request is executed to HDD by using HDD lock password stored in NVRAM and new HDD lock password.

As described above, FIT_CAP.1[2] is realized.

7.11. F.RESET(Authentication Failure Frequency Reset Function)

F.RESET is a function to reset the number of authentication failure counted in each authentication function including the administrator authentication. (Do not relate to the lock is valid or not.)

This function operates by activating TOE such that the main power supply is turned on, it returns from the power failure and so forth. When it starts, the following numbers of authentication failure are reset.

- The number of failure to authentication of administrator
- The number of failure to authentication of a service engineer
- The number of failure that is kept for each user box to authentication of user box

As described above, FIA_AFL.1[1], FIA_AFL.1[2] and FIA_AFL.1[4] are realized.