bizhub C352P / ineo+ 351P / magicolor 8460CK Control Software

Security Target

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

Version：1.04

Issued on：June 1, 2007

Created by：

KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

<Revision History>

Date	Ver.	Division	Approved	Checked	Created	Revision
2006/05/08	1.00	Development Div. 12	Ishida	Nakajima	Yoshida	Initial Version
2006/07/05	1.01	Development Div. 12	Ishida	Nakajima	Yoshida	・Correct the list of option products ・Add the setup function description ・Delete the wrong description about FAX unit connection
2006/11/22	1.02	Development Div. 12	Ishida	Nakajima	Yoshida	・Correct accompanying the revised ST of bizhub C352 / bizhub C300/ ineo$^+$ 351/ ineo$^+$ 300 Control Software (1.04) ・Correction
2007/05/10	1.03	Development Div. 12	Ishida	Nakajima	Yoshida	Correct according to the other model's correction
2007/06/01	1.04	Development Div. 12	Ishida	Nakajima	Yoshida	Correct according to the other model's correction

―【 Contents 】―

― 【 List of Figures 】――――――――――――――――――――――――――――――

― 【 List of Tables 】――――――――――――――――――――――――――――――

1. ST Introduction

1.1. ST Identification

- ST Title : bizhub C352P / ineo$^+$ 351P / magicolor 8460CK Control Software Security Target
- ST Version : 1.04
- CC Version : 2.3
- Created on : June 1, 2007
- Created by : KONICA MINOLTA BUSINESS TECHNOLOGIES, INC. Eiichi Yoshida

1.2. TOE Identification

- TOE Name : Japan：bizhub C352P / ineo$^+$ 351P / magicolor 8460CK Zentai Seigyo Software
Overseas：bizhub C352P / ineo$^+$ 351P / magicolor 8460CK Control Software
- TOE Version : 9J06-0100-GM0-11-000
- TOE Type : Software
- Created by : KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

1.3. CC Conformance Claim

The TOE, which is the subject of this ST, conforms to the following.

- Security function requirement
  Part2 Extended

- Security assurance requirement
  Part3 Conformant

- Evaluation assurance level
  EAL3 Conformant (No additional assurance component)

- PP Reference
  This ST does not carry out a PP reference.

- Reference
  - Common Criteria for Information Technology Security Evaluation Part 1:Introduction and general model 2005 Version 2.3 CCMB-2005-08-001
  - Common Criteria for Information Technology Security Evaluation Part 2:Security functional requirements 2005 Version 2.3 CCMB-2005-08-002
  - Common Criteria for Information Technology Security Evaluation Part 3:Security assurance requirements 2005 Version 2.3 CCMB-2005-08-003
  - Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model August 2005 Version 2.3 CCMB-2005-08-001 (December 2005 Translation Version 1.0, Information-technology Promotion Agency Japan, Security Center)
  - Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements August 2005 Version 2.3 CCMB-2005-08-002 (December 2005 Translation Version 1.0, Information-technology Promotion Agency Japan, Security Center)
  - Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements August 2005 Version 2.3 CCMB-2005-08-003 (December 2005 Translation Version 1.0, Information-technology Promotion Agency Japan, Security Center)
  - Interpretations - 0512 (December 2005 Information-technology Promotion Agency Japan, Security Center, Information Security Certification Office)

1.4. ST Overview

bizhub C352P/ ineo+ 351P / magicolor 8460CK is Konica Minolta Business Technologies, Inc. network printer. (Hereafter, "Printer" as all these generic names) . The target of evaluation (TOE) of this Security Target (ST) is the "bizhub C352P/ ineo+ 351P / magicolor 8460CK Control Software," that controls the entire operation of the printer, including the operation control processing and the image data management that are accepting from the panel of the main body of the printer or through the network. This ST explains the security functions that are realized by the TOE.

TOE offers the protection from exposure of the highly confidential document stored in the printer. Moreover, TOE can encrypt the image data written in HDD for the danger of taking HDD that is the medium that stores the image data in the printer out illegally by installing the encryption board which is the option parts of the printer. Besides, TOE has the deletion method to follow various overwrite deletion standards. It deletes all the data of HDD completely and it contributes to the prevention of the divulging information of the organization that uses the printer by using the method at the time of abandonment or the lease returns.

This ST is the documentation for describing the necessity and sufficiency of these TOE Security Functions.

2. TOE Description

2.1. TOE Type

The bizhub C352P/ ineo+ 351P / magicolor 8460CK Control Software that is the TOE is an embedded software product that controls the operation of whole printer overall in the flash memory on the printer controller.

2.2. Environment for the usage of Printer

Figure 1 shows the expected general environment for the usage of the printer equipped with TOE. Moreover, the matters, assumed in the environment for the usage, show by a run of the item below

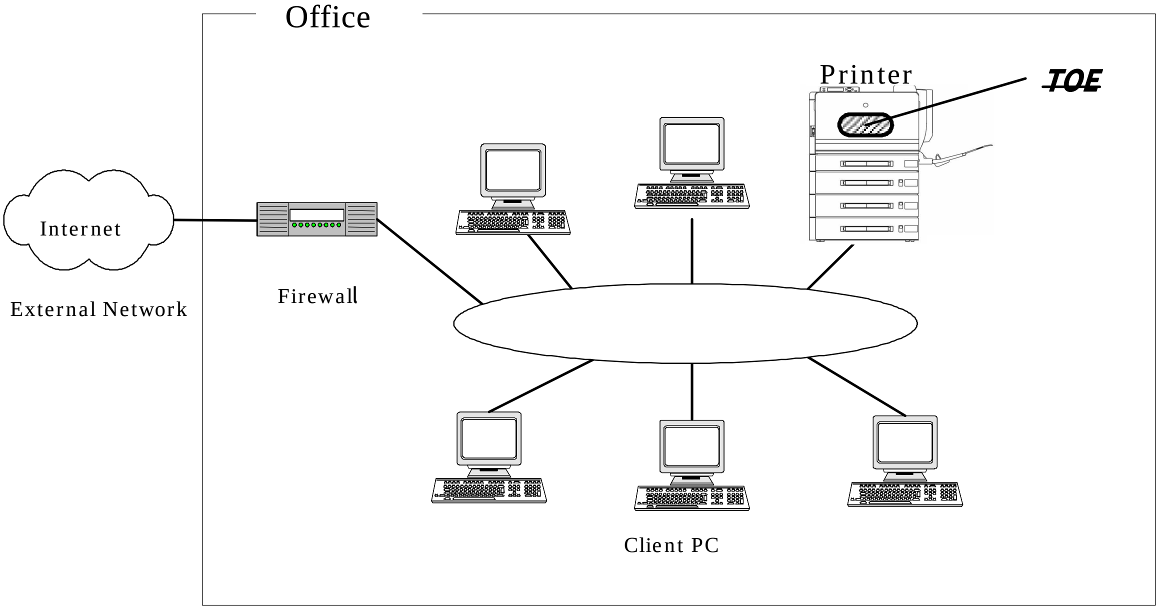

Figure 1 An example of the expected environment for usage of the Printer

- The intra-office LAN exists as a network in the office.
- The printer connects to the client PCs via the intra-office LAN, and has mutual data communication.
- 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 printer from the external network is carried out.
- The intra-office LAN provides a network environment that cannot be intercepted by the office operation including using the switching hub and installing the wiretapping detector.

2.3. Operation Environment of the TOE

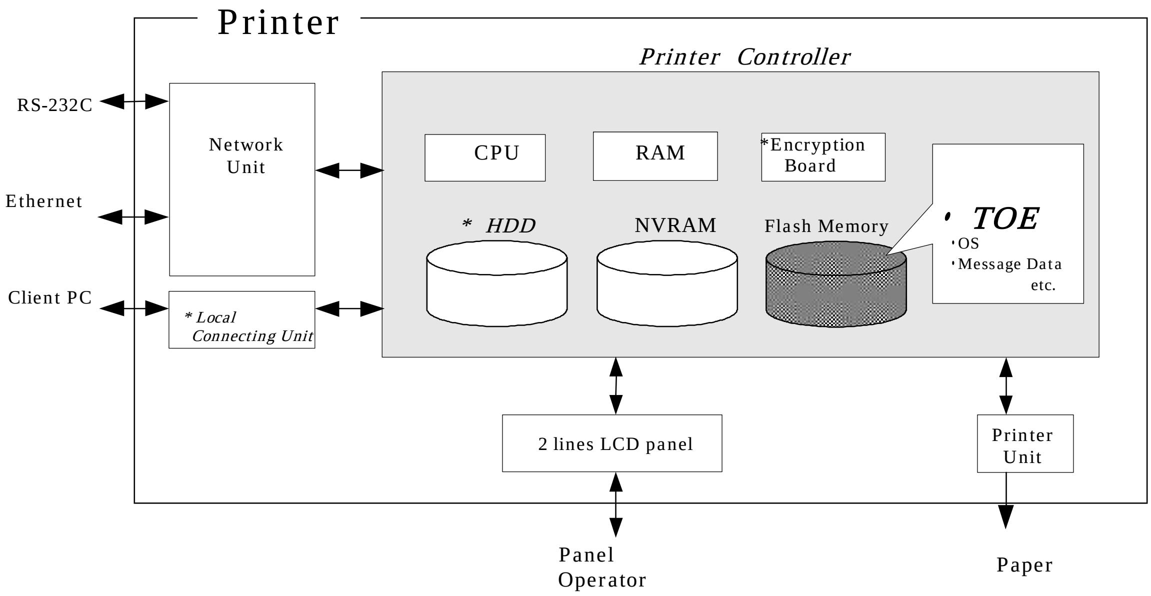

Figure 2 Hardware composition that relates to TOE

Figure2 shows the structure of the hardware environment on the printer that TOE needs for the operation. TOE exists on the flash memory on the printer controller which builds in the body of the printer and is loaded and run on the RAM.

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

- Flash memory
  Storage medium that stores the object code of the “Printer Control Software” that is the TOE. Additionally, it stores the message data of each country’s language to display the response accessed through the panel and network, OS (VxWorks), and so on.

- HDD (※Optional Part)
  Hard disk drive of 40GB in capacity. It is utilized besides the image data is stored as a file, temporarily image data with such as extension conversion, and as an area where the transmission address data kept.
  As a feature function, the security function (HDD lock function) is installed, being possible to set the 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.

- NVRAM
  Nonvolatile Memory. The memory medium that stores various setting values needed for the operation of the printer used for processing of TOE.

- Encryption Board（※Optional Part）
  The hardware-based cryptographic function, which is the integrated circuit for encryption, is installed in order to encipher all data to be written in HDD. It is not pre-installed in printer as standard for convenience' sake of a sale, but is sold as an optional part.

- 2 Lines LCD Panel
  The exclusive control device for the operation of the printer equipped with the 2lines LCD panel of a liquid crystal monitor, ten-key, cursor key, menu/select key, cancel key.

- Main power supply
  The power switch for activating Printer

- Network Unit
  The interface device to connect to the Ethernet. It supports 10BASE-T and 100BASE-TX.

- Local Connecting Unit（※Optional part）
  A unit that uses Print function with local connection by connecting using the client PC and USB or parallel port. According to the circumstances in sales, it is sold as the option part and is not attached on the printer.

- RS-232C
  The serial can be connected through the D-sub9 pin. When breaking down, the maintenance function can be used through this. In addition, it can utilize a remote diagnostic function (later description) to connect with the modem connected with the public circuit.

2.4. Role of the TOE User

The roles of the personnel that relate to the use of the printer with the TOE are defined as follows.

- User
  Printer’s user who performs a printing from PC by using printer.（In general, the employee in the office is assumed.）

- Administrator
  Printer's user who carries out the management of the operation of the printer. An administrator performs the operation management of the printer and the management of users. (In general, it is assumed that the person elected from the employees in the office plays this role.）

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

- Person in charge at the Organization that uses the printer
  A person in charge at the organization that manages the office where the printer is installed. This person assigns an administrator who carries out the management of the operation of the printer.

- Person in charge at the Organization that manages the Maintenance of the printer
  A person in charge at the organization that carries out management of the maintenance for the printer. This person assigns service engineers who perform the maintenance management for the printer.

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

2.5. Functions provided by the TOE

A user uses a variety of functions of the TOE from the panel and a client PC via the network. The following explains typical functions, such as the basic function, the user box function to manage the image files stored, the user identification and authentication function, the administrator function manipulated by administrator, the service engineer function manipulated by service engineer, and the function operated in the background without the user's awareness.

2.5.1. Basic Function

In Printer, the function to accept the print from PC exists, and TOE performs the core control in the operation of these functions. It converts the raw data acquired from the external device of the printer controller into the image file, and registered in RAM and HDD. (After two or more conversion processing is done, the compression conversion is done as for the print image file from PC.) The image file which has been compressed is decompressed into data for the print or for the transmission, and is transmitted to the device outside of the printer controller concerned.

Operations of print is managed by the unit of job, and can be cancelled the operation, by the command from the panel.

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

- Secure Print Function
  When the secure print password is received with the printing data, the image file is stored as the standby status. And the print command and password input from the panel allows printing.
  This function, in the printing operation by the PC, removes the possibility that other users stole a glance at the printing of high-leveled confidential data and lost it into the other printings.

2.5.2. User Box Function

The directory named “user box” can be created as an area to store the image file in HDD. The access of a user is controlled by the password set for the user box.

TOE processes the following required operation, against the user box or the image file in a user box for an operation requests that is transmitted from the panel or the network unit through a network from a client PC.

- Print of image file in a user box, move and copy it to other user boxes
- Deletion of the image file in the user box,
- Storage period setting of image file in the user box (Delete automatically after the period passes.)
- Change of the user box name, change of the password, and deletion of the user box, etc.

2.5.3. Administrator Function

TOE provides the functions such as the management of the 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 function related to the security.

- Management of user box settings
  - Registration and change of user box password
- Management of network setting
  - IP address, NetBIOS name and AppleTalk printer name etc.
- Backup and restore function of NVRAM and HDD
  - It is performed through the network by using an application exclusive use for the management installed in the client PC.
- Complete overwrite deletion function of HDD
  - There is the data deletion method conformed to various military standards.
  - When it's started, in conformity with a set method, the overwrite deletion is executed for all area of HDD.
- Format function of HDD
  - A logical format is executable.

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

- Setting of a password policy function
  - Select ON or OFF for the function to check the several conditions of the password, such as the valid number of digits for the various passwords, etc.
- Setting of the authentication method of secure print and the prohibit function of authenticating operations.
  - There are the mode that the authentication operation prohibition function operates for the authentication of the secure print, and the mode not done.
  - The operation mode of the function that the failure authentication in each authentication function detects the failure synchronizes, too.
  - Selecting the above-mentioned operational mode

- Setting of the network setting modification function by SNMPv1 and v2.
  - Select the permission or the prohibition of the modification operation function of MIB by SNMPv1 and v2
- Setting of HDD lock function
  - Selecting ON or OFF.
  - Register or change the HDD lock password when ON is selected.
- Setting of encryption function（※only when the encryption board installed）
  - Selecting ON or OFF.
  - Register or change the Encryption passphrase when ON is selected.
- Setting of user box collective management function
  - Select the permission or the prohibition for the user box collective management function.
- Setting of the print capture function
  - A function to verify the print data received by MFP when print function breaks down.
  - Selecting ON or OFF for the above-mentioned function.
- Setting of network setting management reset function
  - A network setting management reset function resets a series of items in a factory default.
  - Selecting permission or prohibition for the above-mentioned function.

2.5.4. Service Engineer Function

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

- Modification function of administrator password

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

- Setting of remote diagnostic function (later description)
  - Able to select permission or prohibition.
- Setting of a TOE update function via Internet
  - Able to select permission or prohibition.
- Setting of maintenance function
  - Able to select permission or prohibition.
- The format function of HDD
  - A logical format and a physical format are executable.
- Installation setting of HDD
  - An explicit installation setting is necessary to use HDD as a data storage area.
- Initialization function
  - The various setting values that the user or the administrator has set and the data that the user has stored are deleted.

2.5.5. 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 Encryption key generation function

When the encryption board, an optional product, is installed in printer controller, the encoding and decoding is processed on the encryption board due to the reading and writing data in HDD. (TOE does not process the encryption and description itself.)

The operation setting of this function is performed by the administrator function. When it operates, TOE generates the encryption key by the encryption passphrase that was entered on the panel.

② HDD Lock Function

HDD has the HDD lock function as measure against the illegal taking out, when the password is set.

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

③ Remote diagnostic function

Making use of several connected systems such as E-mail, and a modem connection through a RS-232C, in communication with support center of printer produced by Konica Minolta business technologies Ltd., it manages the state condition of printer and the machinery information such as frequency of printing. In addition, if necessary, appropriate service (shipment of an additional toner, the account claim, dispatch of the service engineer due to the failure diagnosis, etc.) is provided.

④ Updating function of TOE

TOE facilitated with the function to update itself. As for the update means, there are a method that exists as one of items of remote diagnostic function, a method that downloads from FTP server through Ethernet (TOE update function via Internet), and a method that performs the connection of the Compact Flash memory medium.

⑤ Setup function

It offers the function to setup by using the installed software dedicated to perform on PC with connecting to client PC through RS-232C. It especially shows the operation setting function related to the behaviour of security function in this setup function. Dedicated installed software is used by service engineer and so it’s not offered to a user.

- ✧ Setting of remote diagnostic function (later description)
  - Able to select permission or prohibition
- ✧ Setting of a TOE update function via Internet
  - Able to select permission or prohibition
- ✧ Setting of maintenance function
  - Able to select permission or prohibition
- ✧ The format function of HDD
  - A logical format and a physical format are executable
- ✧ Installation setting of HDD
  - An explicit installation setting is necessary to use HDD as a data storage area
- ✧ Initialization function

- The various setting values that the user or the administrator has set and the data that the user has stored are deleted

2.5.6. 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, there is the reset function of the network setting and the update function of TOE through the network, but the use of these functions is prohibited.

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 CE password should be set along with the password policy.

- Setting of password policy function : Valid
- Setting of secure print authentication method
  : Authentication operation prohibition function effective method (In conjunction with it, it becomes in the state of the panel lock for five seconds at the time of the authentication failure in the panel. And it becomes the account lock (Failure frequency threshold: 1-3 times) as well.)
- Setting of user box collective management function
  : Prohibit
- Setting of the network setting modification function with SNMPv1 and v2
  : Prohibit
- Setting of HDD lock function : Valid
- Setting of Encryption function : Valid
- Setting of print capture function : Prohibit
- Setting of maintenance function : Prohibit
- Remote diagnostic function : Prohibit
- Network setting management reset function
  : Prohibit
- TOE update function via Internet : Prohibit

The following function becomes the setup status showing below with the timing enabling the enhanced security function. Unlike above functions, it is possible to change the setting individually. However, when the setting is enabled, this has the system to report that status on the 2 lines LCD panel for not satisfying the enhanced security conditions.

- Setup function : Prohibit

3. TOE Security Environment

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

3.1. Concept of Protected Assets

Security concept of TOE is "the protection of data that can be disclosed against the intention of the user". As printer is generally used, the following image file in available situation becomes the protected assets. (The following image files are able to be handled only when HDD is installed. It's assumed that the option HDD is installed on the printer in TOE security environment.)

- Secured print file
  - ➢ image file registered by secured print
- User Box file
  - ➢ image file stored in the personal user box and public user box)

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.

In the print of the secure print file and the transmission of the user box file, making in the preparation for the threat thought when illegal printer or mail server is connected by any chance, the setting of printer (IP address etc.) requires not to be modified illegally. Therefore, the setting of printer (IP address etc.) is considered as subsidiary protected assets.

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

- Secure Print File
- User Box File
- On Memory Image File
  - ➢ Image file of job in the wait state
- Stored Image File
  - ➢ Stored image files other than secure print file and user box file
- Remaining Image File
  - ➢ The file which remains in the HDD data area that is not deleted only by general deletion operation (deletion of a file maintenance area)
- File related to the Image
  - ➢ Temporary data file generated in print image file processing

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 printer）

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

A.SECRET（Operational condition about secret information）

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

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

Printer 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.

T.DISCARD-PRINTER（Lease-return and disposal of Printer）

When the leaser returned or the discarded printer were collected, secure print file, a user box file, on memory image file, the stored image file, the remaining image file, the image-related file, and the set various passwords (administrator password, SNMP password, HDD lock password, encryption passphrase, secure print password, user box password) can leak by the person with malicious intent taking out and analyzing an HDD in printer.

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

- A secure print file, a user box file, a on-memory image file, a stored image file, a remaining image file, an image-related file, and the set-up various passwords (secure print password, user box password) can leak by a person or a user with malicious intent illegally taking out and analyzing an HDD in printer.
- A person or a user with malicious intent illegally replaces an HDD in printer. In the replaced HDD, new files of the secure print file, a user box file, on-memory image file, a stored image file, a remaining image file, an image related file, and set various passwords are

accumulated. A person or a user with malicious intent takes out and analyzes the replaced HDD and image files 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 which is not permitted to use by printing a user box file

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

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

T.ACCESS-NET-SETTING（An unauthorized change of network setting）

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

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

The possibility of leaking a user box file and secure print file rises because malicious person or user changes the settings related to the enhanced security function.

T.BACKUP-RESTORE（Unauthorized use of Backup function and restoration function）

The user box file and the secure print file can leak by malicious person or user using the backup function and the restoration function illegally. Also highly confidential data such as password can be exposed and each setting values are falsified.

3.4. Organizational Security Policies

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

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.

4.1. Security Objectives for the TOE

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

O.BOX（User box access control）

- TOE permits the user functions of the user box and the user box file in the user box only to the user who is permitted the use of this user box.

O.SECURE-PRINT（Secure print file access control）

TOE permits the print of the secure print file only to the user who is permitted the use of this secure print file.

O.CONFIG（Access limitation to management function）

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

- The setting function related to the network address of printer
- Backup function
- Restoration function

TOE permits the operations of the following functions only to the administrator and the service engineer.

- The function related to the setting of Enhanced Security function

O.OVERWRITE-ALL（Complete overwrite deletion）

TOE overwrites all data regions of HDD in printer by using the data for deletion, and makes impossible the restoration of all the image data. In addition, TOE offers a function to initialize a setting value such as the highly confidential password on NVRAM that is set by a user or an administrator. (Administrator password, SNMP password, HDD lock password, Encryption Passphrase)

O.CRYPT-KEY（Encryption key generation）

TOE generates the encryption key to encrypt and store all data including the image file written in HDD in printer.

O.CHECK-HDD（Validity confirmation of HDD）

TOE verifies that the correct HDD is installed.

4.2. Security objectives for the environment

In this section, the security objectives for the environment, in the environment of the usage of the TOE, is identified and described being divided into the IT environment security objectives and the non-IT environment security objectives.

4.2.1. IT environment security objectives

OE.CRYPT（Encryption of HDD）

An encryption board installed in printer encrypts all data including an image file to be written in the HDD inside printer and then stores it to the HDD.

OE.LOCK-HDD（Access control of HDD）

An HDD installed in printer accepts reading out of data only from the printer where this HDD is installed.

OE.FEED-BACK（Feedback of password）

The application of a browser etc. used by client PC to access printer offers the appropriate feedback protected for input the user box password and administrator password.

4.2.2. Non-IT environment security objective

OE-N.ADMIN（A reliable administrator）

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

OE-N.SERVICE（The service engineer's guarantee）

・The person in charge in the organization that carries out the maintenance management of the printer educates a service engineer in order to faithfully carry out the given role for the installation of the TOE, the set up of TOE and the maintenance of a printer with TOE.

・The administrator observes the maintenance work of a printer with TOE by a service engineer.

OE-N.NETWORK（Network Environment in which the printer is connected）

・The person in charge in the organization who uses the printer carries out the tapping prevention measures by setting the cipher communications equipment and the tapping detection equipment to the LAN of the office where the printer with TOE is installed.

・The person in charge in the organization who uses the printer 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 the printer with TOE.

OE-N.SECRET（Appropriate management of confidential information）

The administrator has the user implement the following operation.

・Keep the user password and secure print password confidential.

・Keep the user box password confidential between the user who commonly utilizes 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 them promptly.

The administrator executes the following operation.

- Should not set the value that can be guessed for the administrator password, SNMP password, the HDD lock password and encryption passphrase.
- Keep the administrator password, the SNMP password, the HDD lock password, and the encryption passphrase confidential.
- The administrator password, the SNMP password, the HDD lock password, and the encryption Passphrase should be properly changed.

The service engineer executes the following operation.

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

OE-N.SESSION（Termination of session after operation）

The administrator has the user implement the following operation.

- After the operation of the secure print file and the operation of user box and user box file end, the logoff operation is performed.

The administrator executes the following operation.

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

The service engineer executes the following operation.

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

OE-N.SETTING-SECURITY（Operation setting of Enhanced Security function）

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

5. IT Security Requirements

In this chapter, the TOE security requirements and IT environment security requirements are described.

<Definition of Label>

The security function requirements required for the TOE and IT environment 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. In addition, [E] is added at the end of a label of a requirement needed in IT environment in order to state it clearly whether an object of each requirement is TOE or IT environment.

< 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. (The number to indicate the repetition is added with separating respectively by TOE requirement and IT environmental requirement.)

<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.

5.1. TOE Security Requirements

5.1.1. TOE Security Function Requirements

5.1.1.1. 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*] : ***Konica Minolta Encryption specification standard***	
[assignment: *cryptographic key generation algorithm*] : ***Konica Minolta HDD Encryption key generation algorithm (SHA-1)***	
[assignment: *cryptographic key sizes*] : ***128bit***	
Hierarchical to :	No other components
Dependencies :	FCS_CKM.2 or FCS_COP.1（FCS_COP.1[E])、FCS_CKM.4（N/A)、FMT_MSA.2（N/A)

5.1.1.2. 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 「Table1 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 1 User Box Access Control Operational List

Subject	Object	Operational List
A task to act for a user	*User Box File*	***・Print*** ***・Move to other user boxes*** ***・Copy to other user boxes*** ***・Backup***

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 「Tabel2 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 2 Secure Print File Access Control: Operational List

Subject	Object	Operational list
A task to act for a user	*Secure Print File Access Control*	***・Print*** ***・Back-Up***

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 3 Setting management access control operational list」

[assignment: *access control SFP*]：
Setting management access control

Hierarchical to ： No other components
Dependencies ： FDP_ACF.1（FDP_ACF.1[3]）

Table 3 Setting Management Access Control: Operational List

Subject	Object	Operational list
A task to act for a user	• *HDD Lock Password Object* • *Encryption passphrase Object*	• *Settings* • *Back-Up* • *Restore*
	• *Printer Address Group Object* [1]	• *Settings* • *Restore*

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 Attributes （User Box ID）* • *Administrator Attributes*

＜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 print, move to other user boxes and copy to the other user boxes, to the user box file that have the matched user box attributes with the user box attributes (user box ID) of the subject attributes.***
- ***A task to act for a user who has an administrator attribute is permitted to backup a user box file.***

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 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[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:

[1] The Printer address group object is a series of data concerning the address of the main body of printer such as IP address and the Appletalk printer name.

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 substituted for a user	⇒	***・File attributes（Secure print internal control ID）*** ***・Administrator attributes***

＜Object＞		***＜Object attributes＞***
・Secure print file	⇒	***・File attributes（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 a file attribute (the secure print internal control ID) is permitted the print operation to the secure print file that has matched the 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] ：

A task to act for a user who has an administrator attribute is permitted to back up secure print file.

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 substituted for a user	⇒	***・Administrator attributes*** ***・CE attributes***

＜Object＞

・HDD Lock Password Object

・Encryption passphrase object

・Printer address group object

[assignment: *access control SFP*]：

Setting management 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 act for a user who has an administrator attribute is permitted to set the HDD lock password object and the encryption passphrase object, and then to operate the restoration and back-up.***
- ***A task act for a user who has an administrator attribute is permitted to set the printer address group object, and to operate the restoration.***
- ***A task act for a user who has a CE attribute is permitted to set the HDD lock password object and the encryption passphrase 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）

5.1.1.3. 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 CE password.***

[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[assignment: range of acceptable values] : an administrator configurable positive integer within 1～3

FIA_AFL.1.2[1]

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].

[assignment: *list of actions*]：
＜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 CE password.***
- ***If it's not under the authentication status, lock the authentication function which uses the CE 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[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 the 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: range of acceptable values]：an administrator configurable positive integer within 1～3***
FIA_AFL.1.2[2]
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].
[assignment: *list of actions*] ： ***＜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 MIB object through SNMP***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] ***[assignment: range of acceptable values]：an administrator configurable positive integer within 1～3***
FIA_AFL.1.2[3]
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].
[assignment: *list of actions*]： ***＜Action when it is detected＞*** ***Deny the access to the MIB object and lock the authentication function to use SNMP password.*** ***＜Operation for recovering the normal condition＞*** ***• Perform the lock release function offered within the administrator mode.*** ***• Reboot the TOE.***
Hierarchical to ： No other components
Dependencies ： FIA_UAU.1（FIA_UAU.2[2]）

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 secure print file***
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] ***[assignment: range of acceptable values]：an administrator configurable positive integer within 1～3***

FIA_AFL.1.2[4]

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].

[assignment: *list of actions*]：

＜Action when it is detected＞

Deny the access to the secure print file and lock the authentication function for the concerned secure print file.

＜Operation for recovering the normal condition＞

- ***Perform the lock release function offered within the administrator mode.***
- ***Reboot the TOE.***

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

FIA_AFL.1[5] Authentication failure handling

FIA_AFL.1.1[5]

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: range of acceptable values]：an administrator configurable positive integer within 1～3

FIA_AFL.1.2[5]

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].

[assignment: *list of actions*]：

＜Action when it is detected＞

Deny the access to the user box and the user box file in the concerned user box and lock the authentication function for the concerned user box.

＜Operation for recovering the normal condition＞

- ***Perform the lock release function offered within the administrator mode.***
- ***Reboot the TOE.***

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

FIA_AFL.1[6] Authentication failure handling

FIA_AFL.1.1[6]

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 when it accesses service mode***
- ***Authentication when it accesses administrator mode from the panel***
- ***Authentication when it accesses secure print file***
- ***Authentication when it accesses user box from the panel***

[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

[assignment: positive integer number] ：1

FIA_AFL.1.2[6]

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].

[assignment: *list of actions*]：

＜Action when it is detected＞

Deny all access from the panel.

＜Operation for recovering the normal condition＞

- ***Automatically release the lock after 5 seconds.***

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_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）***

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, CE Password)*** meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]：

- ***Number of digits: 8- digits***
- ***Character type: ASCII code（0x21 ～ 0x7E、except 0x22 and0x2B）***
- ***Rule ：① Do not composed by only the same kind of character strings.***
  ② Do not set the same password as the current setting.

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 ***(SNMP Password)*** meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]：

- ***Number of digits: 8- digits***
- ***Character type: ASCII code 0x20 ～ 0x7E）***

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 passphrase)*** meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]：

- ***Number of digits: 20- digits***
- ***Character type: ASCII code（0x21 ～ 0x7E、except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E,***

0x5B, 0x5C and 0x5D）

- ***Rule ： Do not composed by only the same kind of character strings.***

.

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 <u>secrets</u> ***(Secure print password, User box password)*** meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]：

- ***Number of digits: 8- digits***
- ***Character type: ASCII code（0x20 ～ 0x7E、 except 0x22 and0x2B）***
- ***Rule ： Do not composed by only the same kind of character strings.***

Hierarchical to ： No other components

Dependencies ： No dependencies

FIA_SOS.1[5] Verification of secrets

FIA_SOS.1.1[5]

The TSF shall provide a mechanism to verify that <u>secrets</u> ***(Session Information)*** meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]：

10^{10} and above

Hierarchical to ： No other components

Dependencies ： No dependencies

FIA_SOS.2 TSF Generation of secrets

FIA_SOS.2.1

The TSF shall provide a mechanism to generate secrets ***(Session information)*** that meet [assignment: *a defined quality metric.*].

[assignment: *a defined quality metric.*]：

$10^{10}$and above

FIA_SOS.2.2

The TSF shall be able to enforce the use of TSF generated secrets for [assignment: *list of TSF functions*].

[assignment: *list of TSF functions*]：

- ***Administrator authentication （Access through the network）***
- ***User box authentication （Access through the network）***

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 <u>user</u> ***(Service Engineer)*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that <u>user</u> ***(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 the user box)* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user *(User who is permitted to use the 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 CE password.***
- ***When the administrator changes the HDD lock setting.***
- ***When the administrator changes the Encryption function setting.***

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)***	
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*]: ***・For user box attributes, 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 ***• For file attributes, 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.***		
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

5.1.1.4. Security management

FMT_MOF.1[1]		**Management of security functions behaviour**
FMT_MOF.1.1[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*** ***• Service Engineer***		
Hierarchical to	：	No other components
Dependencies	：	FMT_SMF.1（FMT_SMF.1）、FMT_SMR.1（FMT_SMR.1[1]、FMT_SMR.1[2]）

FMT_MOF.1[2]		**Management of security functions behaviour**
FMT_MOF.1.1[2]		
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*]： ***• SNMP password authentication function***		
[selection: *determine the behaviour of, disable, enable, modify the behaviour of*] ： ***modify the behaviour of***		
[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_MOF.1[3]		**Management of security functions behaviour**
FMT_MOF.1.1[3]		
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*]： ***• Setup function***		
[selection: *determine the behaviour of, disable, enable, modify the behaviour of*] ： ***enable***		

[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_MSA.3	**Static attribute initialization**
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 authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.	
[assignment: *the authorized 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*] ： ***• SNMP password*** ***• Secure print password*** ***• Threshold Number of authentication failure***	
[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[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*] ： ***User box password of the relevant 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[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*]]： ***modify***
[assignment: *the authorised identified roles*]： ***• Administrator*** ***• Service Engineer***
Hierarchical to ： No other components
Dependencies ： FMT_SMF.1（FMT_SMF.1)、FMT_SMR.1（FMT_SMR.1[1]、FMT_SMR.1[2]）

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*]： ***• SNMP password*** ***• User box password*** ***• Secure print password***
[selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]： ***query***
[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[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*]： ***CE password***
[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[6] Management of TSF data

FMT_MTD.1.1[6]

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, SNMP password

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

[assignment: *the authorised identified roles*]：
Administrator, Service Engineer

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

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
• Operation Setting Function of SNMP password authentication function by administrator
• Setting function of authentication failure frequency threshold by administrator in the authentication operation prohibition function
• Backup Function by administrator [2]
• Restoration Function by administrator [3]
• Deletion Function of detected value of unauthorized access to SNMP 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 SNMP password by administrator
• Modification function of user box password by administrator
• Initialization function of administrator password by administrator
• Initialization function of SNMP password by administrator
• Modification function of CE password by service engineer
• Modification function of administrator password by service engineer
• Start function of Setup function by service engineer
• Stop function of Enhanced Security function by service engineer
• Initialization function of administrator password by service engineer
• Initialization function of SNMP password by service engineer
•Modification function of user box password of the user box by user who is permitted the use of public user box

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

[2] A part of a backup function corresponds to the inquiry function of TSF data.

[3] A part of the restoration function corresponds to the modification function of the TSF data.

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 authorized to use that 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]）

5.1.1.5. Protection of the TSF

FPT_RVM.1 **Non-bypassability of the TSP**
FPT_RVM.1.1
The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
Hierarchical to ： No other components
Dependencies ： No dependencies

FPT_SEP.1 **TSF domain separation**
FPT_SEP.1.1
The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2
The TSF shall enforce separation between the security domains of subjects in the TSC.
Hierarchical to ： No other components
Dependencies ： No dependencies

5.1.1.6. Extended requirement: Identification and approval of access destination

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

Audit：FIA_NEW.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 user identification mechanism including offered user identification information b) Basic　Use all of user identification mechanism including offered user deification information
Management：FIA_NEW.1
The following actions could be considered for the management functions in FMT. a) management of user identification information

5.1.1.7. Extended requirement: Remaining information protection after the explicit deletion operation

FNEW_RIP.1	**Protection of remaining information on the user data and TSF data after explicit deletion operation**
FNEW_RIP.1.1	
TSF shall ensure that each previous information contents assigned to the resource is made unavailable by the explicit deletion of the following objects and TSF data.: [assignment: *list of object and list of TSF data*].	
[assignment : *List of object and list of TSF data*]： ***＜Objects＞*** ***・User Box file*** ***・Secure print file*** ***・On memory image file*** ***・Stored image file*** ***・Remaining image file*** ***・Image-related file*** ***・HDD lock password object*** ***・Encryption passphrase object*** ***＜TSF data＞*** ***・Administrator password*** ***・SNMP password*** ***・User Box password*** ***・Secure print password*** ***・Remaining TSF data***[4]	
Hierarchical to	：　No other components
Dependencies	：　No dependencies

[4] TSF data remaining in the HDD data area, that cannot be deleted only by the deletion of the file management area.

Audit：FNEW_RIP.1
Use including the information of user identification performing the explicit deletion operation.
Management：FNEW_RIP.1
There is no foreseen management activity.

5.1.2. Minimum Security Strength of Function

The minimum strength of function level of the TOE is SOF-Basic. The required TOE security functions that use a probabilistic/permutational mechanism are FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.2[4], FIA_UAU.6, FIA_SOS.1[1], FIA_SOS.1[2], FIA_SOS.1[3], FIA_SOS.1[4], FIA_SOS.1[5] and FIA_SOS.2.

Encryption key generation algorithm of FMT_CKM.1 is not included in the object of the minimum strength of function level.

5.1.3. 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 4 TOE Security Assurance Requirements

TOE Security Assurance Requirements		Component
Class ACM: Configuration management	CM capabilities	ACM_CAP.3
	CM scope	ACM_SCP.1
Class ADO: Delivery and Operation	Delivery	ADO_DEL.1
	Installation, generation and start-up	ADO_IGS.1
Class ADV: Development	Function specification	ADV_FSP.1
	High-level design	ADV_HLD.2
	Representation correspondence	ADV_RCR.1
Class AGD: Guidance Documents	Administrator guidance	AGD_ADM.1
	User guidance	AGD_USR.1
Class ALC: Life Cycle Support	Development security	ALC_DVS.1
Class ATE: Tests	Coverage	ATE_COV.2
	Depth	ATE_DPT.1
	Functional tests	ATE_FUN.1
	Independent testing	ATE_IND.2
Class AVA: Vulnerability Assessment	Misuse	AVA_MSU.1
	Strength of TOE security functions	AVA_SOF.1
	Vulnerability analysis	AVA_VLA.1

5.2. Security Requirements for the IT environment

5.2.1.1. Cryptographic support

FCS_COP.1[E] Cryptographic operation

FCS_COP.1.1[E]

The TSF ***(Encryption board)***、shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

[assignment: *list of standards*]：
FIPS PUB 197

[assignment: *cryptographic algorithm*]：
AES

[assignment: *cryptographic key sizes*]：
128bit

[assignment: *list of cryptographic operations*]：
・Encryption of all data written in HDD
・Decryption of all data read from HDD

Hierarchical to	：	No other components
Dependencies	：	FDP_ITC.1 or FCS_CKM.1（FCS_CKM.1)、FCS_CKM.4（N/A)、 FMT_MSA.2（N/A)

5.2.1.2. Identification and Authentication

FIA_AFL.1[E] Authentication failure handling

FIA_AFL.1.1[E]

The TSF ***（HDD）*** 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 by HDD Lock function at the time of accessing HDD

[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[assignment: positive integer number] ：5

FIA_AFL.1.2[E]

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].

[assignment: *list of actions*]：
＜Action when it is detected＞
Deny the reading and writing of data to HDD.
＜Operation for recovering the normal condition＞
Turn off electricity to HDD（Power OFF）

Hierarchical to	：	No other components
Dependencies	：	FIA_UAU.1（FIA_UAU.2[E])

FIA_UAU.2[E] User authentication before any action

FIA_UAU.2.1[E]

The TSF ***（HDD）*** shall require each user ***（The main body of Printer where HDD installed）*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user ***（The main body of Printer where HDD installed）***.

Hierarchical to	：	FIA_UAU.1
Dependencies	：	FIA_UID.1（N/A)

FIA_UAU.7[E]	**Protected authentication feedback**
FIA_UAU.7.1[E]	
The TSF *（PC application）* shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.	
[assignment: *list of feedback*] ： ***display "*" in every character data input***	
Hierarchical to ：	No other components
Dependencies ：	FIA_UAU.1（FIA_UAU.2[2]、FIA_UAU.2[4]）

6. TOE Summary Specification

6.1. TOE Security Functions

The list of the TOE security function led from the TOE security function requirement is shown in the following Tables 5. The detailed specification is explained in the paragraphs described below.

Table 5: The list of the name and identifier of TOE Security function

No.	TOE Security Function	
1	F.ADMIN	Administrator function
2	F.ADMIN-SNMP	SNMP administrator function
3	F.SERVICE	Service mode function
4	F.USER	User function
5	F.BOX	User box function
6	F.PRINT	Secure print function
7	F.OVERWRITE-ALL	Overwrite all area function
8	F.CRYPT	Encryption key generation function
9	F.HDD	HDD validation function
10	F.RESET	Authentication Failure Reset function

6.1.1. 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.)

6.1.1.1. Administrator identification authentication function

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

- Offers the administrator authentication mechanism authenticating by the administrator password that consists of the character shown in Table 6.
  - Offers the administrator authentication mechanism using the session information besides the administrator password, after the administrator is authenticated to the access from the network,
  - According to protocol, use the session information of more than 10^{10}, or generate and use the session information more than 10^{10}.
- Return “*" for each character as feedback for the entered administrator password.
- Resets the number of authentication failure when succeeding in the authentication.
- In the case of access from a panel, it doesn't accept the input from a panel for five seconds when failing in the authentication.

- Locks all the authentication functions to use the administrator password when detecting the authentication failure that becomes 1〜3 times at total in each authentication function by using the administrator password. (Refuse the access to the administrator mode)
  - ➢ The administrator specifies the failure frequency threshold by the unauthorized access detected threshold setting function.
- Lock of Authentication function is released with F.RESET function operated.

Table 6 Character and number of digits used for password

Objectives	Number of digits	Characters
CE Password	8-digits	92 characters in total can be selected ASCII code（0x21 - 0x7E, except 0x22 and 0x2B） ・Number：0 - 9 ・Alphabet：Capital letter and small letter ・Symbols：!, #, $, %, &, ' , (,), *, , , - , . , / , : , ; , <, =, >, ?, @, [, ¥ ,] , ^ , _ , ` , { , | , } , ~
Administrator Password		
User Box Password	8-digits	93 characters in total can be selected ASCII code（0x20 - 0x7E, except 0x22 and 0x2B） ・Number：0 - 9 ・Alphabets：Capital letter and small letter ・Symbols：! , # , $, % , & , ' , (,) , * , , , - , . , / , : , ; , < , = , > , ? , @ , [, ¥ ,] , ^ , _ , ` , { , | , } , ~ , *SPACE*
Secure Print Password		
HDD Lock Password	20-digits	83 characters in total can be selected ASCII code（0x21-0x7E, except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C and 0x5D） ・Number：0 - 9 ・ Alphabets：Capital letter and small letter ・ Symbols：! , # , $, % , & , ’ , * , + , - , . , / , =, ?, @, ^, _ , ` , { , | , } , ~
Encryption passphrase		
SNMP Password ・Privacy Password ・Authentication Password	More than 8-digits	95 characters in total can be selected ASCII code（0x20 - 0x7E） ・Number：0 - 9 ・Alphabets：Capital letter and small letter ・Symbols：! , # , $, % , & , ' , (,) , * , , , - , . , / , : , ; , < , = , > , ? , @ , [, ¥ ,] , ^ , _ , ` , { , | , } , ~ , ” , + , *SPACE*

6.1.1.2. Function offered 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.

① Change of Administrator password

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

- ➢ Offers the administrator password authentication mechanism that is authenticated by the administrator password which consists of the character shown in Table 6.

- ➢ 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 by the access from the panel.
- ➢ When the authentication failure that becomes 1-3 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.)
  - The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- ➢ Lock of Authentication function is released with F.RESET function operated.
- ➢ 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 6.
  - It shall not be composed of one kind of character.
  - It doesn't match with the current value.

② User Box Settings

- ➢ User Box Registration
  - Set the user box password to the selected unregistered user box ID and register the user box.
  - 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 6.
    - ✧ It shall not be composed of one kind of character.
- ➢ Change of User Box Password
  - The user box password set to 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 6.
    - ✧ It shall not be composed of one kind of character.

③ Release of Lock

Reset (0 clear) the number of authentication failure for all users.

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

Reset (0 clear) the number of authentication failure of all user boxes.

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

Reset (0 clear) the number of authentication failure of SNMP password.

- ➢ If there is a MIB object to which access is locked, the lock is released.

④ Setting of unauthorized access detection threshold

The unauthorized access detection threshold in the authentication operation prohibition function is set for 1-3 times.

⑤ Setting and execution of all area overwrite deletion function

The deletion method shown in the following table is selected first, and then the overwrite deletion at the data area of an HDD is performed. (Perform F.OVERWRITE-ALL.)

Table 7 A type of overwrite deletion of all area and the method of overwriting

Method	Overwritten data type and their order
Mode:1	0x00
Mode:2	Random numbers ⇒ Random numbers ⇒ 0x00
Mode:3	0x00 ⇒ 0xFF ⇒Random numbers ⇒Verification
Mode:4	Random numbers ⇒ 0x00 ⇒ 0xFF
Mode:5	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF
Mode:6	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒Random numbers
Mode:7	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA
Mode:8	0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0x00 ⇒ 0xFF ⇒ 0xAA ⇒ Verification

⑥ Network Settings

A setup operation of the following setting data is performed.

- A series of setup data that relates to The printer address（IP address, NetBIOS Name, AppleTalk Printer Name, etc.）

⑦ Execution of back-up and restoration function

All the setting data stored in an NVRAM and an HDD is backed-up and re-stored except the administrator password and the CE password.（possible to set by a unit of medium）As the object related to security, due to the relation of confidentiality and completeness, the one shown by the following classifications is targeted.

＜Type A : Object to which back-up and restoration should be limited＞

- HDD lock password
- Encryption passphrase
- SNMP password
- Secure print password
- User Box password

＜Type B : Object to which restoration should be limited＞

- A series of data that relates to the Printer address setting
- Setting data of Enhanced Security function
- Authentication failure frequency threshold of authentication operation prohibition function

＜Type C : Object to which back-up should be limited＞

- Secure print file
- User box file

⑧ Operation setting function of HDD lock function

＜Operation Setting　ON＞

When turning it ON from OFF, it verifies that the newly set HDD lock password satisfies the following qualities.

- It is composed of the characters and by the number of digits shown in Table 6.
- It shall not be composed of one kind of character.

＜Modification of HDD lock password＞

Change the HDD lock password. By using the HDD lock password currently set, when it is re-authenticated as an administrator, and the new password satisfies the quality, it is changed.

- Offers the HDD lock password verification mechanism that verified the HDD lock password that consists of the character shown in Table 6.
- Return, in verification, “*" for each character as feedback for the entered 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 6.
  - It shall not be composed of one kind of character.

⑨ Operation setting of encryption function

When an optional encryption board is installed to The printer, it can be operated.

＜Operation Setting　ON＞

When turning it ON from OFF, it verifies that the encryption 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 Table 6.
- It shall not be composed of one kind of character.

＜Encryption Passphrase Change＞

Change the encryption passphrase. By using the encryption passphrase currently set, when it is re-authenticated as an administrator, and the new encryption passphrase satisfies the quality, F.CRYPT is performed.

- Offers the encryption passphrase verification mechanism that verified the encryption passphrase that consists of the character shown in Table 6.
- Return, in verification, “*" for each character as feedback for the entered encryption passphrase.
- Verify the encryption passphrase newly set if the following qualities are satisfied.
  - It is composed of the characters and by the number of digits shown in Table 6.
  - It shall not be composed of one kind of character.

⑩ Function related to Enhanced Security function

The function that influences the setting of the Enhanced Security function that the administrator operates is as follows. (* It has explained the influence of the backup and restoration function in ⑦.)

- Operation setting of Enhanced Security function

  Function to set valid or invalid of Enhanced Security function.
- HDD logical format function

  Function to re-write system file of OS in HDD. Along with the execution of this logical format, the setting of the Enhanced Security function is invalidated.
- Overwrite deletion function for all area

  The settings of enhanced security function are invalidated by executing the overwrite deletion of all area

⑪ Change of SNMP password

The SNMP password (Privacy password and Authentication password) is changed. Verify that the SNMP password newly set satisfies the following qualities.

- ➢ It is composed of the characters and by the number of digits shown in Table 6.

⑫ Setting of SNMP password authentication function

The authentication method in the SNMP password authentication function is set to "Only Authentication password" or the "Authentication password and Privacy password".

6.1.2. F.ADMIN-SNMP（SNMP administrator function）

F.ADMIN-SNMP is a security function, which identifies and authenticates the administrator in the access through the network by using SNMP from PC, and then permits the operation of a setting function of the network only to the administrator whose identification and authentication was succeeded.

6.1.2.1. Identification and authentication function by SNMP password

It identifies and authenticates by the SNMP password, that the user who accesses the MIB object through the network with the use of SNMP is an administrator

- Offers the SNMP authentication mechanism which authenticates by the SNMP password that consists of the character shown in chart 6.
  - ➢ Only Authentication password or both the Privacy password and the Authentication password is used.
  - ➢ In the case of SNMP, the SNMP password is used for every session without requiring the administrator authentication mechanism by the separate session information.
- Reset the authentication failure frequency if it succeeds in authentication.
  - ➢ In the case of both the Privacy password and the Authentication password are used, the authentication failure frequency is reset only when both passwords together succeeded in the authentication.
- When the authentication failure that becomes the 1-3 times at total in each authentication function by using the SNMP password is detected, all the authentication functions to use the SNMP password are locked.（The access to the MIB object is refused.）
  - ➢ The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
  - ➢ In the case of both the Privacy password and the Authentication password are utilized, even though both passwords together fails in authentication, it is detected as one failure.
- To release the lock, the lock release function to the MIB object of F.ADMIN is performed or the F.RESET function operates.

6.1.2.2. Management function using SNMP

When it is identified and authenticated that the user is an administrator by the SNMP password, the access to the MIB object is permitted, and then the operation of the setting data shown as followings is permitted to be done.

① Network Settings

Setting operation of the following setting data is performed.

- ➢ A series of setting data that relates to The printer address（IP address, NetBIOS name, AppleTalk printer name, etc.）

② Change of SNMP password

The SNMP password (Privacy password and Authentication password) is changed. Verify that the SNMP password newly set satisfies the following qualities.

- ➢ It is composed of the characters and by the number of digits shown in Table 6.

③ Setting of SNMP password authentication function

The authentication method in the SNMP password authentication function is set to the "Authentication password only" or the "Privacy password and the Authentication password".

6.1.3. 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 CE password and the administrator password.

6.1.3.1. 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.

- ● Offers the CE authentication mechanism that is authenticated by the CE password that consists of the character shown in Table 6.
  - ➢ The CE authentication mechanism by the separate session information is not required because the service mode can only be accessed from the panel.

- ● Return “*" for each character as feedback for the entered CE password.
- ● Resets the number of the authentication failure when succeeding in the authentication.
- ● Not accept the input from the panel for five seconds when the authentication failed.
- ● When the authentication failure that becomes 1-3 times at total in each authentication function by using the CE password is detected, it locks all the authentication functions to use the CE password. (The access to the service mode is refused.)
  - ➢ The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- ● Lock of authentication function is released with F.RESET function operated.

6.1.3.2. Function offered 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 CE password

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

- ➢ Offers the CE authentication mechanism that is re-authenticated by the CE password that consists of the characters shown in Table 6.
- ➢ Resets the number of authentication failure 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 1-3 times at total in each authentication function by using the CE password is detected, it logoffs the service mode accessing from the panel, and locks all the authentication functions to use the CE password. (The access to the service mode is refused.)
  - ・ The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- ➢ The F.RESET function operates to release the lock of the authentication function.
- ➢ It verifies that the CE password newly set satisfies the following qualities.
  - ・ It is composed of the characters and by the number of digits, shown in the Table 6.
  - ・ It shall not be composed of one kind of character.
  - ・ It shall not be matched with the current value.

② Change of administrator password

Change the administrator password. Verify that the administrator password newly set satisfies the following qualities.

- ➢ It is composed of the characters and by the number of digits, shown in the Table 6.
- ➢ It shall not be composed of one kind of character.
- ➢ It shall not be matched with the current value.

③ Function that relates to Enhanced Security function

The functions that influence the setting of the Enhanced Security function that the service engineer operates are as follows.

- ➢ HDD logical format function

  Function to re-write system file of OS in HDD. The setting of the Enhanced Security function is invalidated along with the execution of this logical format.
- ➢ HDD physical format function

  A function to rewrite the entire disk in HDD with a regulated pattern including the signal rows such as the track and sector information. The setting of the Enhanced Security function is invalidated along with the execution of this physical format.
- ➢ HDD installation setting function

  Function to make the installed HDD effective. The setting of the Enhanced Security function is invalidated by nullifying this HDD installation setting.
- ➢ Initialization function

  Function to reset every setting value written in NVRAM to the factory default. The setting of the Enhanced Security function is invalidated by executing this initialization function.

④ Function that sets the operation of setup function

Set whether or not to use (operate) the setup function.

⑤ Function that relates to password initialization function

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

- Initialization function

  Function to reset various setting values written in NVRAM to the factory default. The administrator password and the SNMP password are set to an initial value of the factory shipment by executing this initialization function. Both of the operation settings of the HDD lock function and the encryption function are turned OFF. (The HDD lock password and the encryption passphrase have been set cannot be used again by turning OFF the setting operation.)

- HDD physical format function

  A function to rewrite the entire disk to a regulated pattern in HDD including the signal rows such as the track and sector information. The HDD lock function is turned OFF along with the execution of this physical format. (The HDD lock password that is set cannot be used again by turning OFF the operation setting.)

6.1.4. F.BOX（User Box Function）

F.BOX is a series of security function related to the user box, such as the access control function to permit various operations of the concerned user box and the user box file after the user is identified and authenticated that you are the registered user in the access to the user box

6.1.4.1. Registration of user box

- Register the user box by setting the user box password to the selected unregistered user box ID.
- Verify that a user box password registered satisfies the following conditions.
  - It is composed of the characters and by the number of digits, shown in the Table 6.
  - It shall not be composed of one kind of character.

6.1.4.2. Authentication function in access to user box

For the access request for each user box, after, the user who accesses is authenticated that it is a user permitted the use of a user box concerned respectively.

- Offers the user box authentication mechanism that is authenticated by the user box password that consists of the character shown in Table 6.
  - After the user box is authenticated to the access from the network, it offers the user box authentication mechanism using the session information besides the user box password.
- According to protocol, it utilizes the 10^{10} session information or more, or generated and uses the 10^{10} session information or more.
- Return “*" for each character as feedback for the entered user box password.
- Resets the number of authentication failure when succeeding in the authentication.
- In case of the access from the panel, when it fails in the authentication, an input from the panel is not accepted for five seconds.
- When the authentication failure that becomes the 1-3 times in total is detected for the user box concerned, the authentication function to the user box concerned is locked.
- The administrator specifies the failure frequency threshold by the unauthorized access

detection threshold setting function.

- The lock of the authentication function is released by the lock release function to the user box of F.ADMIN executed or by the operation of the F.RESET function.

6.1.4.3. Access control to a user box file in a user box

The task to act for the user who is permitted to use the user box is related the "User Box ID" of the user box as a user box attribute. This task is permitted the user box file, which has a corresponding user box attribute to the user box attribute of a task, to do the printing, the movement to other user boxes, and the copy operations to other user boxes.

6.1.4.4. Change of user box password

Change the user box password of the user box. When the user box password newly set satisfies the following qualities, it is changed.

- It is composed of the characters and by the number of digits shown in Table 6.
- It shall not be composed of one kind of character.

6.1.5. 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 user to use the secure print file for the access to the secure print file from the panel.

6.1.5.1. Authentication function by the 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.

- Offers the secure print authentication mechanism that is authenticated by the secure print password that consists of the character shown in Table 6.
  - The secure print authentication mechanism by the separate session information is not needed because it becomes only an access from the panel in the case of the secure print.
- Return “*" for each character as feedback for the entered secure print password.
- Resets the number of authentication failure when succeeding in the authentication.
- The access from the panel is not accepted for 5 seconds when the authentication is failed.
- When the authentication failure that becomes the 1-3 times in total for the secure print file concerned is detected, the authentication function to the secure print file is locked.
  - The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- The lock is released by the lock release function to the secured print file of F.ADMIN executed or the operation of the F.RESET function.

6.1.5.2. Access control function to a secure print file

The task to act for the user who is identified and authenticated has the authenticated secure print internal control ID 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.

6.1.5.3. Registration function of a secure print file

Following process is performed for the registration request of the secure print file.

① Registration of the secure print password
The registered secure print password is verified to meet the following requirements.

- ➢ It is composed of the characters and by the number of digits shown in Table 6.
- ➢ 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.

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

F.OVERWRITE-ALL executes the overwrite deletion in the data area of HDD and initializes the setting value of the password that is set to NVRAM as well. The object for the deletion or the initialization is as follows.

＜Object for the deletion：HDD＞

- ● Secure print file
- ● User box file
- ● On memory image file
- ● Stored image file
- ● Remaining image file
- ● Image related file
- ● User box password
- ● Secure print password
- ● Remaining TSF data

＜Object for the initialization：NVRAM＞

- ● Administrator Password
- ● SNMP password
- ● Operation setting of HDD lock function（OFF）
- ● Operation setting of Encryption function（OFF）

The deletion methods such as the data written in HDD and the written frequency is executed according to the deletion method of all area overwrite deletion function set in F.ADMIN (Table 7). The HDD lock password and the encryption passphrase cannot be used for being turned off the operation setting of the HDD lock function and the encryption function. The setting of the Enhanced Security function becomes invalid in the execution of this function. (Refer to the description for the operation setting of the Enhanced Security function in F.ADMIN.)

6.1.7. F.CRYPT（Encryption key generation function）

F.CRYPT is generated the encryption key to encrypt all data written in HDD by using the HDD encryption key generation algorithm (SHA-1) that is regulated by the Konica Minolta encryption specification standard. Konica Minolta HDD encryption key generation algorithm (SHA-1) is the algorithm to generate the encryption key by using the SHA-1 regulated by FIPS 180-1.

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

6.1.8. F.HDD（HDD verification function）

F.HDD is a check function to permit reading from and writing in the HDD only when it is verified that the illegal HDD is not installed and is confirmed validity when the HDD lock password is set to HDD

When the HDD lock password is set to HDD, the status of HDD is confirmed in the HDD operation verifying at the time of TOE starting. When the HDD lock password certainly being set is returned as the result of status confirmation, the access to HDD is permitted. If the HDD lock password not being set is returned, the access to HDD is refused because of an illegitimate possibility.

6.1.9. 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 object account locked is released.)

- The number of failure to authentication of administrator
- The number of failure to authentication using SNMP password
- The number of failure to authentication of service engineer
- The number of failure to authentication of each user box
- The number of failure to authentication of each secure print

6.2. TOE Security Strength of Function

The TOE security functions having probabilistic/permutational mechanisms are as follows. The strength of each of the functions satisfies the SOF-Basic.

① Administrator authentication mechanism, HDD lock password verification mechanism, and encryption passphrase verification mechanism which F.ADMIN offers

② CE authentication mechanism which F.SERVICE offers

③ Secure print authentication mechanism which F.PRINT offers

④ User box authentication mechanism which F.BOX offers

⑤ SNMP authentication mechanism which F.ADMIN-SNMP offers

6.3. Correspondence between TOE Security Functions and Function Requirements

The correspondence between TOE security function and TOE security function requirements shows in Table 13 of 8.3 Rational for TOE Summary Specification. Table 13 shows that the TOE security function corresponds to at least one TOE security function requirement.

6.4. Assurance Measures

The following table shows the assurance measures to meet the component of the TOE security assurance requirements for EAL3 that are stipulated in Table 8.

Table 8 Correspondence between TOE Assurance Requirements and assurance measures

TOE Security Assurance Requirement		Component	TOE Security Assurance Requirement
Class ACM: Configuration management	CM capabilities	ACM_CAP.3	・Configuration management plan ・Configuration List ・CM record
	CM scope	ACM_SCP.1	
Class ADO: Delivery and Operation	Delivery	ADO_DEL.1	Delivery instructions
	Installation, generation and start-up	ADO_IGS.1	・Service Manual bizhub C352P Service Manual [Security Function]（Japanese）、bizhub C352P / ineo+ 351P / magicolor 8460CK Service Manual [Security Function]（English） ・User’s Guide bizhub C352P User’s Guide [Security Operations]（Japanese）、bizhub C352P User's Guide [Security Operations]（English）、ineo+ 351P User's Guide [Security Operations]（English）, magicolor 8460CK User’s Guide [Security Operations] (English)
Class ADV: Development	Functional specification	ADV_FSP.1	Security function specifications
	High-level design	ADV_HLD.2	Security high level design specifications
	Representation correspondence	ADV_RCR.1	Representation correspondence analysis report
Class AGD: Guidance Document	Administrator guidance	AGD_ADM.1	・Service Manual bizhub C352P Service Manual [Security Function]（Japanese）、bizhub C352P / ineo+ 351P / magicolor 8460CK Service Manual [Security Function]（English） ・User’s Guide bizhub C352P User’s Guide [Security Operations]（Japanese）、bizhub C352P User's Guide [Security Operations]（English）、ineo+ 351P User's Guide [Security Operations]（English）, magicolor 8460CK User’s Guide [Security Operations] (English)
	User Guidance	AGD_USR.1	
Class ALC: Life Cycle Support	Development security	ALC_DVS.1	Development security instructions
Class ATE: Test	Coverage	ATE_COV.2	Coverage analysis report
	Depth	ATE_DPT.1	Depth analysis report
	Functional tests	ATE_FUN.1	Test specification and results report

TOE Security Assurance Requirement		Component	TOE Security Assurance Requirement
	Independent testing	ATE_IND.2	Printer control software including TOE
Class AVA: Vulnerability Assessment	Misuse	AVA_MSU.1	※ no specific document （Reflected in the guidance documents）
	Strength of TOE security functions	AVA_SOF.1	Vulnerability analysis report
	Vulnerability analysis	AVA_VLA.1	

7. PP Claims

There is no conformance to a PP in this ST.

8. Rational

8.1. Security Objectives Rationale

8.1.1. 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 9 Conformity of Security Objectives to assumptions and Threats

Assumption/Treat Security objectives	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	A.SETTING	T.DISCARD-PRINTER	T.BRING-OUT-STORAGE	T.ACCESS-BOX	T.ACCESS-SECURE-PRINT	T.ACCESS-NET-SETTING	T.ACCESS-SETTING	T.BACKUP-RESTORE
O.BOX	▨	▨	▨	▨	▨			●				
O.SECURE-PRINT	▨	▨	▨	▨	▨				●			
O.CONFIG	▨	▨	▨	▨	▨					●	●	●
O.OVERWRITE-ALL	▨	▨	▨	▨	▨	●						
O.CRYPT-KEY	▨	▨	▨	▨	▨		●					
O.CHECK-HDD	▨	▨	▨	▨	▨		●					
OE.CRYPT							●					
OE.LOCK-HDD							●					
OE.FEED-BACK								●	●	●	●	●
OE-N.ADMIN	●											
OE-N.SERVICE		●										
OE-N.NETWORK			●									
OE-N.SECRET				●								
OE-N.SESSION								●	●	●	●	●
OE-S.SETTING-SECURITY						●						

8.1.2. 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-N.ADMIN, the organization that uses the Printer assigns personnel who are reliable in the organization that uses the Printer, 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-N.SERVICE, the organization that manages the maintenance of the Printer educates the service engineer. Also the administrator needs to observe the maintenance of the Printer, so that the reliability of service engineers is assured.

- **A.NETWORK（Network Connection Conditions for the Printer）**
  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-N.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 Printer from the external networks, so that this condition is realized.

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

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

8.1.3. Sufficiency of Threats

The security objectives against threats are described as follows.

- **T.DISCARD-PRINTER（Lease return and disposal of Printer）**

This threat assumes the possibility of leaking information from HDD inside The printer collected from the user.

O.OVERWRITE-ALL is that TOE offers the function to overwrite data for the deletion to all area of HDD, so that the possibility of the threat is removed by executing this function before The printer is collected.

Accordingly, this threat is countered sufficiently.

- **T.BRING-OUT-STORAGE（Unauthorized taking out of HDD）**

This threat assumes the possibility that the image data in HDD leaks by being stolen from the operational environment under The printer used or by installing the unauthorized HDD and taking away with the data accumulated in it.

For the above, the possibility of the threat is removed because at least either of the following two measures is selected by the administrator.

①O.CRYPT-KEY generates the encryption key for TOE to encrypt data to be written in HDD, and the encryption board encodes data by OE.CRYPT.

②OE.LOCK-HDD doesn't permit to read data from any other Printer, as a function of the HDD, but the Printer where this HDD is installed.

In the above-mentioned, when only ② is selected, danger of leaking exists by taking out the another HDD without the function of ② having been secretly replaced. For the above, because the validity of HDD installed by TOE is verified by O.CHECK-HDD, data is not written in the HDD replaced secretly. The possibility of the threat is removed consequently.

Accordingly, this threat is countered sufficiently.

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

This threat assumes the possibility that an unauthorized operation is done by using the user function for the user box which each user uses to store the image file.

The operation of user box and the user box file in a user box is restricted only to the user who is the owner by O.BOX, so that the possibility of the threat is removed.

OE.FEED-BACK regulates to return the protected feedback for the entered password in the user box authentication, and OE-N.SESSION also requires the log-off operation after the operation ends, so that O.BOX are 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 operation of the secure print is limited only to the authorized user by O.SECURE-PRINT, so that the possibility of the threat is removed.

OE.FEED-BACK regulates to return the protected feedback for the entered password in the access authentication to the secure print, and OE-N.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.ACCESS-NET-SETTING（Unauthorized change in network setting ）**

This threat assumes the possibility to use the print function to the unauthorized entity from PC by the user who believes as TOE when the network setting which is related to the address of The printer is modified illegally. 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 feedback protected is returned for the entered password by the administrator's authentication and OE-N.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 file and the secure print file by having been changed the specific function setting which relates to security.

  O.CONFIG regulates that only the administrator is permitted to perform the setting 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 regulates that the feedback protected is returned for the entered password by the administrator's authentication, and OE-N.SESSION is also requested to logoff respectively after the operations of the administrator mode ends, so that O.CONFIG is supported sufficiently.

  Accordingly, this threat is countered sufficiently.

- **T.BACKUP-RESTORE（Unauthorized use of back-up function and restoration function）**

  This threat assumes a possibility that the user box file or the secure print file may leak since the back-up function or the restoration function being illegally used. Moreover, this assumes that because of a leak of confidential data such as the password, the various setting values are falsified and there is a similar possibility that the user box file or the secure print file may leak.

  O.CONFIG regulates that the use of the back-up function and the restoration function is permitted only to the administrator, so that the possibility of the threat is removed.

  OE.FEED-BACK regulates that the protected feedback is returned for the entered password by the administrator authentication and OE-N.SESSION is also requested the log-off operation after the operation ends, and so O.CONFIG is sufficiently supported.

  Accordingly, this threat is countered sufficiently.

8.1.4. Sufficiency of Organizational Security Policies

The organizational security policy is not applied.

8.2. IT Security Requirements Rationale

8.2.1. Rationale for IT Security Functional Requirements

8.2.1.1. 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 10 Conformity of IT Security Functional Requirements to Security Objectives

Security Objective Security Functional Requirements	O.BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.CRYPT-KEY	O.CHECK-HDD	OE.CRYPT	OE.LOCK-HDD	OE.FEED-BACK	※ set.admin	※ set.service
set.admin	●	●	●							▨	▨
set.service	●	●	●							▨	▨
FCS_CKM.1					●		▨	▨	▨		
FDP_ACC.1[1]	●		●				▨	▨	▨		
FDP_ACC.1[2]		●	●				▨	▨	▨		
FDP_ACC.1[3]			●				▨	▨	▨		
FDP_ACF.1[1]	●		●				▨	▨	▨		
FDP_ACF.1[2]		●	●				▨	▨	▨		
FDP_ACF.1[3]			●				▨	▨	▨		
FIA_AFL.1[1]							▨	▨	▨		●
FIA_AFL.1[2]							▨	▨	▨	●	
FIA_AFL.1[3]			●				▨	▨	▨		
FIA_AFL.1[4]		●					▨	▨	▨		
FIA_AFL.1[5]	●						▨	▨	▨		
FIA_AFL.1[6]	●	●					▨	▨	▨	●	●
FIA_ATD.1	●	●					▨	▨	▨		
FIA_SOS.1[1]							▨	▨	▨	●	●
FIA_SOS.1[2]			●				▨	▨	▨		
FIA_SOS.1[3]			●				▨	▨	▨		
FIA_SOS.1[4]	●	●					▨	▨	▨		
FIA_SOS.1[5]	●						▨	▨	▨	●	
FIA_SOS.2	●						▨	▨	▨	●	
FIA_UAU.2[1]							▨	▨	▨		●
FIA_UAU.2[2]			●				▨	▨	▨	●	
FIA_UAU.2[3]		●					▨	▨	▨		
FIA_UAU.2[4]	●						▨	▨	▨		
FIA_UAU.6			●				▨	▨	▨	●	●
FIA_UAU.7	●	●					▨	▨	▨	●	●
FIA_UID.2[1]							▨	▨	▨		●
FIA_UID.2[2]			●				▨	▨	▨	●	
FIA_UID.2[3]		●					▨	▨	▨		
FIA_UID.2[4]	●						▨	▨	▨		
FIA_USB.1	●	●					▨	▨	▨		
FMT_MOF.1[1]			●				▨	▨	▨		
FMT_MOF.1[2]			●				▨	▨	▨		
FMT_MSA.3		●					▨	▨	▨		
FMT_MTD.1[1]	●	●	●				▨	▨	▨	●	●
FMT_MTD.1[2]	●		●				▨	▨	▨		
FMT_MTD.1[3]							▨	▨	▨	●	
FMT_MTD.1[4]			●				▨	▨	▨		

Security Objective Security Functional Requirements	O.BOX	O.SECURE-PRINT	O.CONFIG	O.OVERWRITE-ALL	O.CRYPT-KEY	O.CHECK-HDD	OE.CRYPT	OE.LOCK-HDD	OE.FEED-BACK	※ set.admin	※ set.service
FMT_MTD.1[5]							▨	▨	▨		●
FMT_MTD.1[6]			●				▨	▨	▨	●	
FMT_SMF.1	●	●	●				▨	▨	▨	●	●
FMT_SMR.1[1]			●				▨	▨	▨	●	●
FMT_SMR.1[2]	●	●	●				▨	▨	▨	●	
FMT_SMR.1[3]	●						▨	▨	▨		
FPT_RVM.1	●	●	●			●	▨	▨	▨		
FPT_SEP.1	●	●	●				▨	▨	▨		
FNEW_RIP.1				●			▨	▨	▨		
FIA_NEW.1						●	▨	▨	▨		
FCS_COP.1[E]	▨	▨	▨	▨	▨	▨	●				
FIA_AFL.1[E]	▨	▨	▨	▨	▨	▨		●			
FIA_UAU.2[E]	▨	▨	▨	▨	▨	▨		●			
FIA_UAU.7[E]	▨	▨	▨	▨	▨	▨			●		

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

8.2.1.2. Sufficiency

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

- O.BOX（user box access control）

This security objective limits access to the user box and the user box file in the user box to only the user who owns that user box, and needs various requirements that relate to the access control.

＜User box access control (a user box)＞

In order to operate the user box file in a user box, the user needs to be the one who is permitted to use the user box. FIA_UID.2[4] and FIA_UAU.2[4] identifies and authenticates that it is a user who is permitted the use of the user box.

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

In the case of the failure authentication from the panel, FIA_AFL.1 [6] refuses all input acceptances from the panel for 5 seconds in every failure. When the authentication failure reaches 1-3 times, FIA_AFL.1 [5] logoffs if it's under authentication, and locks the authentication function for that user from then on. This lock status is released by the TOE rebooting or the administrator's release operation.

FMT_MTD.1[1] permits only to the administrator the setting of the threshold of the unauthorized access detection value that is the trial frequency of the failure authentication in

the authentication of the user who is permitted the use of the user box.
When FIA_ATD.1 and FIA_USB.1 relates a user box ID to the task of acting use, FDP_ACC.1[1] and FDP_ACF.1[1] permit the user box file that has a corresponding object attribute to the user box ID of the subject attribute the operation such as a print, a movement to other user box, and a copy to other user box.

＜Management of a user box＞
FMT_MTD.1[2] permits the change in the user box password only to the administrator and the user who is permitted to the use of the user box. FIA_SOS.1[4] verifies the quality of the user box password. Moreover, FIA_SOS.1[5] performs the quality verification of the session information used in the user box authentication via the network, and FIA_SOS.2 secures the quality of the session information which is generated and used.

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

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

＜Role 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.

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

- **O.SECURE-PRINT（Secure print file access control）**

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

＜Secure print file access control＞
As it must be a user who is permitted the use of the secure print file to print it, FIA_UID.2[3] and FIA_UAU.2[3] identifies and authenticates that it is a user who is permitted the use of the secure print file.
FIA_UAU.7 returns “*" for each entered character as feedback protected by the panel and supports the authentication.
FIA_AFL.1 [6] refuses all input acceptances from the panel for 5 seconds in every failure. When the authentication failure reaches 1-3 times, FIA_AFL.1 [4] locks the authentication function for to the concerned secure print file. This lock status is released by the TOE rebooting or the administrator's release operation.
FMT_MTD.1[1] permits only to the administrator the setting of the threshold of the unauthorized access detection value that is the trial frequency of the failure authentication in the authentication of the user who is permitted the use of the secure print file.
When FIA_ATD.1 and FIA_USB.1 relate the secure print internal control ID to the task of acting use, FDP_ACC.1[2] and FDP_ACF.1[2] permit the print operation to the secure print

file that has a 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＞
FIA_SOS.1[4] verifies the quality of the secure print password.

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

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

＜Role and controlling function for each management＞
As the role of doing these managements, FMT_SMR.1[2] maintains an administrator. Moreover, FMT_SMF.1 specifies these management functions.

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

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

This security objective limits the setting related to the IP address of the printer, the setting related to the Enhanced Security function, the backup function and the restorations function to the administrator, and needs various requirements to limit the access to a series of 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 setting for the Printer address group object.

＜Operation limitation of Backup and restoration function＞
When the administrator attribute is related to the task of acting the use, the task of acting the user is permitted the back-up operation of;
・ the user box files by FDP_ACC.1[1] and FDP_ACF.1[1].
・ the secure print files by FDP_ACC.1[2] and FDP_ACF.1[2].
・ the encryption passphrase object and the HDD lock password object by FDP_ACC.1[3] and FDP_ACF.1[3].
In addition, the restoration operation is permitted for
・ the encryption passphrase object, the HDD lock password object and the Printer address group object by FDP_ACC.1[3] and FDP_ACF.1[3].
Moreover, the restoration operation (modifying operation) of the followings is permitted only to the administrator.
・ the Enhanced security setting data by FMT_MOF.1[1].
・ the SNMP password, the authentication failure frequency, the secure print password by FMT_MTD.1[1].

- the user box password by FMT_MTD.1[2].

FMT_MTD.1[4] permits only to the administrator the backup operation (inquiry operation) of the SNMP password, the user box password, and the secure print password.

＜Operational limitation of Enhanced Security function＞

FMT_MOF.1[1] permits only the administrator and service engineer to disable the setting for the enhanced security function. FMT_MOF.1[3] permits only the service engineer to enable the setting for the setup function

＜Management of HDD lock password and encryption passphrase＞

When the administrator attribute is related to the task of acting the user, FDP_ACC.1[3] and FDP_ACF.1[3] permit the setting operation to the HDD lock password object and the encryption passphrase object to the task of acting the user. FIA_SOS.1[3] verifies the quality of the HDD lock password and the encryption passphrase. In order to change the HDD lock password and encryption passphrase, FIA_UAU.6 re-authenticates that a user is an administrator by collating with the registered HDD lock password and encryption passphrase. When the authentication is succeeded, the HDD lock password and the encryption passphrase are allowed to be changed.

Moreover, when the CE attribute is related to the task of acting the user, FDP_ACC.1[3] and FDP_ACF.1[3] permit the setting operation to the HDD lock password object and the encryption passphrase object to the task of acting the user.

＜Necessary requirement for accessing MIB object＞

The Printer address group object exists as an MIB object as well, so that the restriction is necessary even in the access from the SNMP.

FIA_UID.2[2] and FIA_UAU.2[2] identify and authenticate that the user who accesses the MIB object is an administrator.

FIA_AFL.1[3] locks the authentication function to access the MIB object when the failure authentication reaches 1-3 times. This lock is released by the start of TOE or the lock release operation by the administrator.

FMT_MTD.1[1] restricts the threshold setting of the unauthorized access detection value that is the trial frequency of the failure authentication in the administrator authentication using the SNMP password only to the administrator

FMT_MTD.1[1] restricts the change in the SNMP password to the administrator. FIA_SOS.1[2] verifies the quality of the SNMP password.

FMT_MTD.1[6] restricts the initialization of the SNMP password only to the administrator and the service engineer.

FMT_MOF.1[2] restricts the method of the SNMP password authentication function only to the administrator.

＜Necessary requirement to keep the administrator secure＞

⇒ refer to set.admin

＜Necessary requirement to keep the service engineer secure＞

⇒ refer to set.service

＜Role and controlling function for each management＞

As the role of doing these managements, FMT_SMR.1[1] maintains a service engineer and FMT_SMR.1[2] maintains an administrator. Moreover, FMT_SMF.1 specifies these management functions.

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

- **O.OVERWRITE-ALL（Complete over write deletion）**

  This security objective regulates that it deletes all data areas of HDD and initializes the concealed information of NVRAM that is set by the user, and requires various requirements that relate to the deletion.

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

  This security objective regulates that, when the encryption board is installed, 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.

  Using Konica Minolta HDD encryption key generation mechanism (SHA-1) according to Konica Minolta encryption specification standard, FCS_CKM.1 generates the 128bit encryption key. Konica Minolta HDD encryption key generation algorithm is not the general standard algorithm that is recognized, but it is the algorithm using SHA-1 specified with FIPS 180-1, and so this is the algorithm with sufficient strength which does not undermine the entropy of 128 bit, and does not undermine the strength level that is required by security objective. (Refer to chapter 6 TOE summary specification for the description related to this algorithm)

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

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

  This security objective regulates that it verifies the validity of HDD in order to confirm the unauthorized HDD doesn't exist, and needs various requirements that relate to the verification of an external entity from TOE.

  FIA_NEW.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.

- **OE.CRYPT（Encryption of HDD）**

  This security objective regulates that the data stored in HDD is encrypted by the encryption board that is the entity of a necessary IT environment for the security maintenance of TOE, and needs various requirements that relate to the encryption.

  Applying FCS_COP.1[E], the encryption board encodes and decodes all the written data to HDD by the 128bit encryption key using AES that conforms to FIPS PUB 197.

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

- **OE.LOCK-HDD（Access control of HDD）**

  This security objective regulates that it refuses the unauthorized access from the printer other than the one that is set by the HDD which is the entity of a necessary IT environment for the TOE security maintenance, and needs various requirements that verify that it is the right Printer where TOE is installed.

  By FIA_UAU.2[E], HDD authenticates that the entity accessing to HDD is the Printer, which HDD is installed.

  When the failure authentication reaches five times, FIA_AFL.1[E] refuses all the accesses to HDD concerning reading and writing data.

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

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

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

  By FIA_UAU.7[E], 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 ①the set of necessary requirement to keep administrator secure (set.admin), ②the 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 an administrator.

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

FIA_AFL.1[6] refuses, in case of the failure authentication tried from the panel, all the input receipts from the panel for five seconds in every failure. When the failure authentication reaches 1-3 times, FIA_AFL.1[2] locks all the authentication functions that use the administrator password from then on. This lock is released by starting TOE with turning OFF and ON the power supply.

FMT_MTD.1[1] permits only to the administrator the setting of the threshold of the unauthorized access detection value which is the trial frequency of the failure authentication in the administrator authentication.

＜Management of administrator's authentication information＞

FIA_SOS.1[1] verifies the quality of the administrator password. Moreover, FIA_SOS.[5] verifies the quality of session information used to authenticate the administrator via the network, and FIA_SOS.2 secures the quality of session information that is generated and used. FMT_MTD.1[3] restricts the change in the administrator password to the administrator and the service engineer. When the administrator changes the administrator password, FIA_UAU.6 re-authenticates it. In this re-authentication, when the failure authentication reaches 1-3 times, FIA_AFL.1[2] releases the authentication status of the administrator from then on. And it locks all the authentication functions to use the administrator password. This lock is released by starting TOE such as turning OFF and ON the power supply.

Moreover, FMT_MTD.1[6] restricts the initialization of the administrator password to the administrator and the service engineer.

＜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 "*" every one character entered as the feedback protected in the panel, and supports the authentication.

FIA_AFL.1[6] refuses all the input receipts from the panel for five seconds at each failure, and when the failure authentication reaches 1-3 times, FIA_AFL.1[1] locks all the authentication functions to use the CE password. This lock is released by starting TOE such as turning OFF and ON the power supply.

FMT_MTD.1[1] permits only to the administrator the setting of the threshold of the unauthorized access detection value that is the trial frequency of the failure authentication in the service engineer authentication.

＜Management of service engineer's authentication information＞

FIA_SOS.1[1] verifies the quality of the CE password. FMT_MTD.1[5] restricts the change in the CE password to the service engineer. Moreover, FIA_UAU.6 re-authenticates it. In this re-authentication, when the failure authentication reaches 1-3 times, FIA_AFL.1[1] releases the authentication status of the service engineer and locks all the authentication functions to use the CE password. This lock is released by starting TOE such as turning OFF and ON the power supply.

＜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 directly not related to the security measures policy, though it not included in the explanation of the above-mentioned sufficiency. But, they are shown to support the security function requirement which is included in the explanation of the above-mentioned sufficiency in the mutual support described later. 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.

8.2.1.3. Necessity of specified IT security function requirement

In this ST, FNEW_RIP.1 and FIA_NEW.1 is stated as an extended requirement. The necessity that presents these requirements and the validity of the assurance requirement applied in guaranteeing requirements is described as follows.

- Extended requirement：Necessity of FNEW_RIP.1

  Regarding FNEW_RIP.1, FDP_RIP.1 is the closest requirement in the viewpoint of remaining information protection, but the requirement needs to regulate the protection of not only user data, but also the TSF data. And so, it is improper in the function requirement concerned that exists in the class of the user data protection, and it requires the extended requirement.

  ＜Validity of requirement identification structure＞

  Because this requirement doesn't have the corresponding class in the data protection class of integration of no division of the TSF data and the user data, a new class named FNEW was set up, the same family name as the RIP family of the FDP class that indicates the remaining information protection, and clarifies the identification.

  Though the predicted management activity is assumed not to be existed, as for the timing of information assuming not to be able to recycle in the requirement is stipulated concretely, especially, the parameter treated as changeability are not guessed in this requirement. In addition, it is shown that the execution record has been left at the predicted audit activity with the user identification.

  Extended requirement：Necessity of FIA_NEW.1

  Regarding FIA_NEW.1, FIA_UID.1 or FIA_UID.2 is the closest requirement in the viewpoint of identification. But the verification act of HDD doesn't approve the act accessed from an external entity by TOE, but also approve the act that TOE itself assigns to an external entity. It is improper in the function requirement concerned, and the extended requirement is necessary.

  ＜Validity of requirement identification structure＞

  Because this requirement is one of the identification requirements, the family named NEW is set as a family added to the FIA class, and clarifies the identification.

  As an activity that is predicted on management, FIA_UID requirement and similar management items are assumed. Also, an activity that is predicted on audit, FIA_UID requirement and similar audit item are assumed.

8.2.1.4. Assurance validity of specified IT security function requirement

Two specified function requirements (FNEW_RIP.1, FIA_NEW.1) are not the greatly extended concept of the function requirement provided by CC part 2, and high contents of novelty. This is not the one to assume the necessity of presenting the TSP model specially or the possibility of a potential hiding channel in order to evaluate this function requirement accurately.

Therefore, it is possible to assure sufficiently the validity of the function that these functional requirements show by the set of the assurance requirement of EAL3, and a special assurance requirement and the assurance requirement required at EAL4 or higher are not required.

8.2.1.5. Dependencies of the 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 11 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、 FMT_MSA.2	FCS_COP.1[E] ＜The reason not to apply①FCS_CKM.4, ② FMT_MSA.2＞ ① 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. ② TOE does not have the security attribute to be managed for the encryption key, and so it is not necessary to regulate a security attribute that is secure.
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]、 <The reason not to apply FMT_MSA.3> There is no necessity for applying this requirement because the security attribute that requires the secure management for the generated object does not exist. (User box ID can be registered by the arbitrary user.)
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] ＜The reason not to apply FMT_MSA.3＞ There is no necessity for applying this requirement because the object attribute doesn't exist.
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[2]
FIA_AFL.1[4]	FIA_UAU.1	FIA_UAU.2[3]
FIA_AFL.1[5]	FIA_UAU.1	FIA_UAU.2[4]
FIA_AFL.1[6]	FIA_UAU.1	FIA_UAU.2[1]、FIA_UAU.2[2]、FIA_UAU.2[3]、FIA_UAU.2[4]
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_SOS.1[5]	None	N/A
FIA_SOS.2	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]

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
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[1]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[1]、FMT_SMR.1[2]
FMT_MOF.1[2]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2]
FMT_MOF.1[3]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[1]
FMT_MSA.3	FMT_MSA.1、FMT_SMR.1	FMT_MSA.1[1]、FMT_MSA.1[2]、FMT_SMR.1[3]
FMT_MSA.3[2]	FMT_MSA.1、FMT_SMR.1	Neither is applicable. ＜The reason not to apply 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_SMR.1＞ The assignment of FMT_MSA.3.2 is not applicable. FMT_SMR.1 is the dependency that is set relating to the following and so there is no necessity of application.
FMT_MTD.1[1]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2]
FMT_MTD.1[2]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2] 、FMT_SMR.1[3]
FMT_MTD.1[3]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2]
FMT_MTD.1[4]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2]、FMT_SMR.1[4]
FMT_MTD.1[5]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[2]、FMT_SMR.1[3]
FMT_MTD.1[6]	FMT_SMF.1、FMT_SMR.1	FMT_SMF.1、FMT_SMR.1[1]、FMT_SMR.1[2]
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]
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[4]
FPT_RVM.1	None	N/A
FPT_SEP.1	None	N/A
FNEW_RIP.1	None	N/A
FIA_NEW.1	None	N/A
FCS_COP.1[E]	FDP_ITC.1 or FCS_CKM.1、FCS_CKM.4、FMT_MSA.2	FCS_CKM.1 ＜The reason not to apply①FCS_CKM.4、②

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
		FMT_MSA.2> ① 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. ② TOE does not have the security attribute to be managed for the encryption key, it is not necessary to be regulated a security attribute that is secure.
FIA_AFL.1[E]	FIA_UAU.1	FIA_UAU.2[E]
FIA_UAU.2[E]	FIA_UID.1	N/A <The reason not to apply FIA_UID.1> This regulates the access to HDD installed in the Printer. There are no multiple access routes because the access to HDD is done through a general IDE interface. In other words, when the some users access, it is unnecessary for this processing the authentication information that each user accessing is needed, and there is no necessity of the identification of the entity to access.
FIA_UAU.7[E]	FIA_UAU.1	FIA_UAU.2[2]、FIA_UAU.2[4]

8.2.1.6. Mutual Support Correlations of IT Security Functional Requirements

The IT security function requirements to operate effectively other security functional requirements which are not specified in the analysis of the dependencies relation of the functional requirement are shown in the table below.

Table 12 Mutual Support Correlations of IT Security Functional Requirements

N/A：Not Applicable

IT Security Functional Requirement	Functional requirement component that operates other security functional requirements validly			
	①Bypass Prevention	②Interference/ Destruction Prevention	③Deactivation Prevention	④Disabling Detection
FCS_CKM.1	N/A	N/A	FMT_MOF.1[1]	N/A
FDP_ACC.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FDP_ACC.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FDP_ACC.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FDP_ACF.1[1]	FIA_UAU.2[2] FIA_UAU.2[4]	FPT_SEP.1	FMT_MOF.1[1]	N/A
FDP_ACF.1[2]	FIA_UAU.2[2] FIA_UAU.2[3]	FPT_SEP.1	FMT_MOF.1[1]	N/A
FDP_ACF.1[3]	FIA_UAU.2[2] FIA_UAU.2[1]	FPT_SEP.1	FMT_MOF.1[1]	N/A
FIA_AFL.1[1]	N/A	FMT_MTD.1[1]	FMT_MOF.1[1]	N/A

IT Security Functional Requirement	Functional requirement component that operates other security functional requirements validly			
	①Bypass Prevention	②Interference/ Destruction Prevention	③Deactivation Prevention	④Disabling Detection
FIA_AFL.1[2]	N/A	FMT_MTD.1[1]	FMT_MOF.1[1]	N/A
FIA_AFL.1[3]	N/A	FMT_MTD.1[1]	FMT_MOF.1[1]	N/A
FIA_AFL.1[4]	N/A	FMT_MTD.1[1]	FMT_MOF.1[1]	N/A
FIA_AFL.1[5]	N/A	FMT_MTD.1[1]	FMT_MOF.1[1]	N/A
FIA_ATD.1	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[4]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_SOS.1[5]	N/A	N/A	N/A	N/A
FIA_SOS.2	N/A	N/A	N/A	N/A
FIA_UAU.2[1]	FPT_RVM.1	FMT_MTD.1[5]	FMT_MOF.1[1]	N/A
FIA_UAU.2[2]	FPT_RVM.1	FMT_MTD.1[1] FMT_MTD.1[3] FMT_MTD.1[4] FMT_MTD.1[6]	FMT_MOF.1[1]	N/A
FIA_UAU.2[3]	FPT_RVM.1	FMT_MTD.1[1] FMT_MTD.1[4]	FMT_MOF.1[1]	N/A
FIA_UAU.2[4]	FPT_RVM.1	FMT_MTD.1[2] FMT_MTD.1[4]	FMT_MOF.1[1]	N/A
FIA_UAU.6	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UAU.7	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_UID.2[4]	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_USB.1	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MOF.1[1]	N/A	N/A	N/A	N/A
FMT_MOF.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MOF.1[3]	N/A	N/A	N/A	N/A
FMT_MSA.3	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[4]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[5]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_MTD.1[6]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMF.1	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMR.1[1]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMR.1[2]	N/A	N/A	FMT_MOF.1[1]	N/A
FMT_SMR.1[3]	N/A	N/A	FMT_MOF.1[1]	N/A
FPT_RVM.1	N/A	N/A	FMT_MOF.1[1]	N/A
FPT_SEP.1	N/A	N/A	FMT_MOF.1[1]	N/A
FIA_NEW.1	FPT_RVM.1	N/A	FMT_MOF.1[1]	N/A
FNEW_RIP.1	N/A	N/A	N/A	N/A
FCS_COP.1[E]	N/A	N/A	N/A	N/A
FIA_AFL.1[E]	N/A	N/A	N/A	N/A
FIA_UAU.2[E]	N/A	N/A	N/A	N/A
FIA_UAU.7[E]	N/A	N/A	N/A	N/A

① Bypass Prevention

＜By-pass prevention of functional requirement that relates to administrator＞

As for FDP_ACF.1[1] that regulates the user box access control, FDP_ACF.1[2] that regulates the secure print file access control, and FDP_ACF.1[3] that regulates the administrator mode access control, the by-pass prevention is supported by FIA_UAU.2[2] that regulates the administrator's identification and authentication.

Furthermore, because FIA_UAU.2[2] is called by FPT_RVM.1 without fail, the by-pass prevention is supported.

＜By-pass prevention of functional requirement that relates to service engineer＞

As for FDP_ACF.1[3] that regulates the setting management access control, the by-pass prevention is supported by FIA_UAU.2[1] that regulates the service engineer's identification and authentication.

In addition, FIA_UAU.2[1] is called by FPT_RVM.1 without fail, the by-pass prevention is supported.

＜By-pass prevention of functional requirement that relates to user box＞

As for FDP_ACF.1[1] that regulates the user box access control, the by-pass prevention is supported by FIA_UAU.2[4] that authenticates the user is the permitted user to use the user box.

In addition, because FIA_UAU.2[4] that regulates the authentication of the user who is permitted the use of the user box are called by FPT_RVM.1 without fail, and so the by-pass prevention is supported.

＜By-pass prevention of functional requirement that relates to secure print＞

As for FDP_ACF.1[2] that regulates the secure print file access control, the by-pass prevention is supported by FIA_UAU.2[3] that authenticates the authorized user to use the secure print file.

In addition, because FIA_UAU.2[3] that regulates the authentication of the authorized user to use the secure print file are called by FPT_RVM.1 without fail, so that the by-pass prevention is supported.

＜By-pass prevention of validity verification of HDD＞

FIA_NEW.1 that verifies the validity of HDD is called by FPT_RVM.1 without fail, so that the by-pass prevention is supported.

② Interference and Destruction Prevention

＜Maintenance of user box access control＞

By FPT_SEP.1, only the subject of two types such as the authenticated administrator who is assumed by the user box access control and the user who is permitted the use of the authenticated user box, can operate the user box and the user box file.

With two requirements in the above-mentioned, FDP_ACF.1[1] is supported in the prevention of interference and destruction from other illegal subject.

＜Maintenance of secure print file access control＞

FPT_SEP.1 permits the operation of the secure print file only to the two types of subject which are the authenticated administrator who is assumed by the secure print file access control and the user who is permitted the use of authenticated secure print file. FDP_ACF.1[2] is supported in the interference and destruction prevention from other illegal subject.

＜Maintenance of setting management access control＞
Only the subject that acts the authenticates administrator who is assumed by the set management access control and the authenticated service engineer can operate the object regulated for by the setting management access control by FPT_SEP.1, and the prevention of an illegal interference and destruction from other illegal subject are supported for FDP_ACF.1[3].

＜Management of CE password＞
The modification operation of the CE password has been permitted only to the service engineer by FMT_MTD.1[5]. This supports the prevention of unauthorized interference and destruction of FIA_UAU.2[1].

＜Management of administrator password＞
The modification operation of the administrator password is permitted only to the administrator and the service engineer by FMT_MTD.1[3]. The initialization of the administrator password is permitted only to the administrator and the service engineer by FMT_MTD.1[6]. This supports the prevention of unauthorized interference and destruction of FIA_UAU.2[2].

＜Management of SNMP password＞
The modification operation of the SNMP password is permitted to the administrator by FMT_MTD.1[1]. The inquiry operation is permitted to the administrator by FMT_MTD.1[4], and the initialization operation is permitted only to the administrator and the service engineer by FMT_MTD.1[6]. This supports the prevention of unauthorized interference and destruction of FIA_UAU.2[2].

＜Management of secure print password＞
The inquiry operation is permitted only to the administrator by FMT_MTD.1[4]. The modification is permitted only to the administrator by FMT_MTD.1[1]. This supports the prevention of unauthorized interference and destruction of FIA_UAU.2[3].

＜Management of user box password＞
The modification operation is permitted to the administrator and the user who is permitted the use of the user box by FMT_MTD.1[2]. The inquiry operation is permitted only to the administrator by FMT_MTD.1[4]. This supports the prevention of unauthorized interference and destruction of FIA_UAU.2[4].

＜Management of authentication failure frequency threshold＞
The modification operation of the authentication frequency failure threshold which is set in all the authentication activities such as the service engineer authentication, the administrator authentication, the secure print authentication, the user box authentication, and the MIB object access authentication is permitted only to the administrator by

FMT_MTD.1[1]. This supports the prevention of unauthorized interference and destruction of FIA_AFL.1[2], FIA_AFL.1[3], FIA_AFL.1[4], FIA_AFL.1[5].

③ Deactivation Prevention
＜Maintenance of Enhanced Security function＞
FMT_MOF.1[1] permits only to the administrator and the service engineer the operation setting of the Enhanced Security function. The Enhanced Security function influences all the TOE security structures except the all area overwrite deletion function executed by the specified operation of the administrator and quality of session information. This supports the deactivation prevention of all the security functions achieved by the security requirements of TOE except FNEW_RIP.1, FIA_SOS/1[5], FIA_SOS.2, FMT_MOF.1[1].

④ Disabling Detection
The requirement that supports the disabling detection doesn't exist.[5]

8.2.2. Rational for Minimum Strength of Function

The Printer that is loaded with this TOE is connected to an intra-office LAN with appropriately controlled connections with external networks. Therefore, there is no possibility that it is directly attacked by unspecified people via the Internet. As long as it has a strength level that can counter the threat by users who are users of the TOE and a person who can enter the office and not user of the TOE as an agent, it is acceptable, as explicitly described in section 3.3. Therefore, this TOE regulates the security objectives by assuming an unskilled attacker and thus, the selection of the SOF-Basic as the minimum strength of function is reasonable.

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

8.2.4. Consistency rationale for the set of IT security functional requirement

The followings show the rationale in which the IT security requirement with a possibility to compete does not exist.

[5] Though this is not shown in the mutual support analysis, FIA_AFL.1 requirement supports respectively against the attack that aims at the disabling of each authentication function. This is sufficient to maintain the security objective of this TOE. (This content is specified by the dependency analysis.)

<IT security functional requirement>

- Though several access control policies are set up by repeating the access control requirement (FDP_ACC.1 etc.), it regulates the access control related to the followings, such as ① user box, ② secure print, ③ Printer addresses. These do not cover each other the same controlled object by several policies, and so they do not compete each other.
- FNEW_RIP.1 is applied as an extended requirement that regulates the deletion of the protective assets, but the threat concerning the possibility of an unauthorized deletion is not targeted in this case because of the concept of emphasis on confidentiality. Therefore, the requirement for the competing data deletion protection has not been selected at all.
- The structure, that a competition possibility is suggested, doesn't exist from the relations between requirements by dependency, correlation by mutual support, and the various analysis of validity of security functional requirement to TOE security objectives.

<IT security assurance requirement>

- EAL that is the assurance package is applied. Therefore, it is confirmed that the possibility of the competition between security assurance requirements doesn't exist regardless of this ST.

8.3. Rational for TOE Summary Specifications

8.3.1. Rational for the TOE Security Functions

8.3.1.1. Necessity

The conformity of the TOE security functions and the TOE security functional requirements are shown in the following table. It shows that the TOE security functions correspond to at least one TOE security functional requirement.

Table 13 Conformity of TOE Security Functions to TOE Security Functional Requirements

TOE Security Function TOE Security Functional Requirement	F.ADMIN	F.ADMIN-SNMP	F.SERVICE	F.BOX	F.PRINT	F.OVERWRITE-ALL	F.CRYPT	F.HDD	F.RESET
FCS_CKM.1							●		
FDP_ACC.1[1]	●			●					
FDP_ACC.1[2]	●				●				
FDP_ACC.1[3]	●	●	●						
FDP_ACF.1[1]	●			●					
FDP_ACF.1[2]	●				●				
FDP_ACF.1[3]	●	●	●						
FIA_AFL.1[1]			●						●
FIA_AFL.1[2]	●								●
FIA_AFL.1[3]	●	●							●
FIA_AFL.1[4]	●				●				●
FIA_AFL.1[5]	●			●					●

TOE Security Function TOE Security Functional Requirement	F.ADMIN	F.ADMIN-SNMP	F.SERVICE	F.BOX	F.PRINT	F.OVERWRITE-ALL	F.CRYPT	F.HDD	F.RESET
FIA_AFL.1[6]	●		●	●	●				
FIA_ATD.1				●	●				
FIA_SOS.1[1]	●		●						
FIA_SOS.1[2]	●	●							
FIA_SOS.1[3]	●								
FIA_SOS.1[4]	●			●	●				
FIA_SOS.1[5]	●			●					
FIA_SOS.2	●			●					
FIA_UAU.2[1]			●						
FIA_UAU.2[2]	●	●							
FIA_UAU.2[3]					●				
FIA_UAU.2[4]				●					
FIA_UAU.6	●		●						
FIA_UAU.7	●		●	●	●				
FIA_UID.2[1]			●						
FIA_UID.2[2]	●	●							
FIA_UID.2[3]					●				
FIA_UID.2[4]				●					
FIA_USB.1				●	●				
FMT_MOF.1[1]	●		●						
FMT_MOF.1[2]	●	●							
FMT_MOF.1[3]			●						
FMT_MSA.3					●				
FMT_MTD.1[1]	●	●							
FMT_MTD.1[2]	●			●					
FMT_MTD.1[3]	●		●						
FMT_MTD.1[4]	●								
FMT_MTD.1[5]			●						
FMT_MTD.1[6]	●		●						
FMT_SMF.1	●	●	●	●					
FMT_SMR.1[1]			●						
FMT_SMR.1[2]	●	●							
FMT_SMR.1[3]				●					
FPT_RVM.1	●	●	●	●	●			●	
FPT_SEP.1	●	●	●	●	●				
FNEW_RIP.1						●			
FIA_NEW.1								●	

8.3.1.2. Sufficiency

The TOE security functions for the TOE security functional requirements are described.

- **FCS_CKM.1**

FCS_CKM.1 regulates the various conditions of the encryption key generated along with the encryption of HDD.

F.CRYPT generates the encryption key of 128bit by using Konica Minolta HDD encryption key generation algorithm (SHA-1).

Accordingly, this functional requirement is satisfied.

- **FDP_ACC.1[1]**

  FDP_ACC.1[1] regulates the relationship between the subject controlled to the user box and the user box file which are the object, and the operation.

  F.ADMIN performs the user box access control for the task of acting for the user to back-up the user box file.

  F.BOX performs the user box access control for the task of acting for the user to print a user box file, mover to other user box, and copy to other user box.

  Accordingly, this functional requirement is satisfied.

- **FDP_ACC.1[2]**

  FDP_ACC.1[2] regulates the relationship between the subject controlled to the secure print file that is the object and the operation.

  F.ADMIN performs the secure print file access control for the task of substituting the user to back up the secure print file.

  F.PRINT performs the secure print file control for the task of substituting the user to print the list of secure print file.

  Accordingly, this functional requirement is satisfied.

- **FDP_ACC.1[3]**

  FDP_ACC.1[3] regulates the relationship between the subjects controlled to the HDD lock password object, Encryption passphrase object, and Printer address group object which are the object and the operation.

  F.ADMIN performs the setting management access control for the task of substituting the user to set, back-up and restore the HDD lock password object and encryption passphrase object. In addition, it performs the setting management access control for the task of substituting the user to set and restore Printer address group object.

  F.ADMIN-SNMP performs the setting management access control for the task of substituting the user to set Printer address group object.

  F.SERVICE performs the setting management access control for the task of substituting the user to set HDD lock password object and encryption passphrase object.

  Accordingly, this functional requirement is satisfied.

- **FDP_ACF.1[1]**

  FDP_ACF.1[1] regulates the regulation of relationship between the subject controlled to the user box file which are an object, and the operation.

  F.ADMIN performs the user box access control to which the following rules are applied.

  ➢ It permits the administrator the back-up operation of the user box file.

  F.BOX performs the user box access control to which the following rules are applied.

  ➢ It permits the user the operation of the user box file in the selected user box such as the print, the movement and the copy.

  Accordingly, this functional requirement is satisfied.

- **FDP_ACF.1[2]**

FDP_ACF.1[2] regulates the regulation of the relationship between the subject controlled to the secure print file which is the object, and the operation.

F.ADMIN performs the secure print file access control to which the following rules are applied.

- It permits the administrator the backup operation of the secure print file.

F.PRINT performs the secure print file access control to which the following rules are applied.

- It permits the printing operation of the selected secure print file to the user who is allowed to use the secure print file.

Accordingly, this functional requirement is satisfied.

- **FDP_ACF.1[3]**

FDP_ACF.1[3] regulates the regulation of the relationship between the subject controlled to the HDD lock password object, the encryption passphrase object and the Printer address group object that are the object, and the operation.

F.ADMIN performs the setting management access control to which the following rules are applied.

- It permits the administrator the setting, the back-up and the restoration of the HDD lock password object and the encryption passphrase object.
- It permits the administrator the setting and the restoration operations of the Printer address group object.

F.ADMIN-SNMP performs the secure print file access control to which the following rules are applied.

- It permits the administrator the setting operation of the Printer address group object.

F.SERVICE performs the setting management access control to which the following rules are applied.

- It permits the service engineer the setting operation of the HDD lock password object and the encryption passphrase object (initialization operation).

Accordingly, this functional requirement is satisfied.

- **FIA_AFL.1[1]**

FIA_AFL.1[1] regulates the action for the authentication failure to the service engineer authentication. In the service engineer authentication for accessing the service mode or changing the CE password, when the authentication failure of failure frequency threshold (1-3 times) that the administrator set is detected, F.SERVICE logs off from the service mode authentication status and locks the authentication function.

F.RESET releases the lock status by the reboot of TOE by turning OFF and ON the power supply that clears the times of failure in each authentication function.

Accordingly, this functional requirement is satisfied.

- **FIA_AFL.1[2]**

FIA_AFL.1[2] regulates the action of the authentication failure to the administrator authentication. In the administrator authentication for accessing the administrator mode or changing the administrator password, when the authentication failure of failure frequency threshold (1-3 times) that the administrator set is detected, F.ADMIN logs off from the authentication status to the administrator mode and locks the authentication function.

F.RESET releases the lock status by the reboot of TOE by turning OFF and ON the power supply that clears the times of failure in each authentication function.

Accordingly, this functional requirement is satisfied.

- **FIA_AFL.1[3]**

  FIA_AFL.1[3] regulates the action for the authentication failure to the administrator authentication when accessing to the MIB object by using SNMP. In the authentication using the SNMP password for accessing to the MIB object, when the authentication failure of failure frequency threshold (1-3 times) that the administrator set is detected, F.ADMIN-SNMP denies the access to the MIB object and locks an authentication function.

  F.RESET releases the lock status by the reboot of TOE by turning OFF and ON the power supply that clears the times of failure in each authentication function.

  Accordingly, this functional requirement is satisfied.

- **FIA_AFL.1[4]**

  FIA_AFL.1[4] regulates the action for the authentication failure to the authentication of the user permitted the use of the secure print file.

  In the authentication of a user permitted the use of the secure print file, when the authentication failure of failure frequency threshold (1-3 times) that an administrator sets is detected, F.PRINT denies the access to the secure print file and locks an authentication function.

  F.RESET releases the lock status by the reboot of TOE by turning OFF and ON the power supply that clears the times of failure in each authentication function. Moreover, F.ADMIN releases the lock status by the lock release function that is available in the administrator mode.

  Accordingly, this functional requirement is satisfied.

- **FIA_AFL.1[5]**

  FIA_AFL.1[5] regulates the action for the authentication failure to the authentication of the user permitted the use of the user box.

  In the authentication for accessing the user box and changing a user box password, when the authentication failure of failure frequency threshold (1-3 times) that an administrator sets is detected, F.BOX denies the access to the user box and locks an authentication function.

  F.RESET releases the lock status by the reboot of TOE by turning OFF and ON the power supply that clears the times of failure in each authentication function. Moreover, F.ADMIN releases the lock status by the lock release function that is available in the administrator mode.

  Accordingly, this functional requirement is satisfied.

- **FIA_AFL.1[6]**

  FIA_AFL.1[6] regulates the action for the authentication failure to the various authentication on the panel. In the authentication of service engineer for accessing the service mode, when the authentication failure is detected, F.SERVICE denies all input receipts from a panel.

  F.ADMIN rejects all input receipts from a panel when the authentication failure is detected in the administrator authentication for accessing the administrator mode.

  F.BOX rejects all input receipts from a panel when the authentication failure is detected in the authentication for accessing to the user box from a panel.

  F.PRINT rejects all input receipts from a panel when the authentication failure is detected in the authentication of a user permitted the use of the secure print file.

These series of operation is released automatically in five seconds.

Accordingly, this functional requirement is satisfied.

- **FIA_ATD.1**

  FIA_ATD.1 regulates the security attribute related by the user.

  F.BOX assigns a user box ID to the task of substituting the user.

  F.PRINT assigns the secure print internal control ID to the task of substituting the user.

  Accordingly, this functional requirement is satisfied.

- **FIA_SOS.1[1]**

  FIA_SOS.1[1] regulates the quality of the administrator password and the CE password.

  F.ADMIN verifies the quality of the administrator password that is composed of ASCII code (0x21-0x7E, except 0x22 and 0x2B) in total of 92 characters by eight digits, is not composed of one kind of character and does not correspond to the value currently set.

  F.SERVICE verifies the quality of CE password and the administrator password that is composed of ASCII code (0x21-0x7E, except 0x22 and 0x2B) in total of 92 characters with eight digits, is not composed of one kind of characters and does not correspond to the value currently set.

  Accordingly, this functional requirement is satisfied.

- **FIA_SOS.1[2]**

  FIA_SOS.1[2] regulates the quality of the SNMP password.

  F.ADMIN verifies that the quality of the SNMP password (Privacy password, Authentication password) is composed of ASCII code (0x20-0x7E) in total of 95 characters by eight or more digits. F.ADMIN-SNMP also verifies that the quality of the SNMP password (Privacy password, Authentication password) is composed of ASCII code (0x20-0x7E) in total of 95 characters with eight or more digits.

  Accordingly, this functional requirement is satisfied.

- **FIA_SOS.1[3]**

  FIA_SOS.1[3] regulates the quality of the HDD lock password and the encryption passphrase.

  F.ADMIN verifies that the quality of the HDD lock password and the encryption passphrase is composed of ASCII code (0x21-0x7E, except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C, 0x5D) in total of 83 characters by 20 digits, and is not composed of one kind of characters.

  Accordingly, this functional requirement is satisfied.

- **FIA_SOS.1[4]**

  FIA_SOS.1[4] regulates the quality of the secure print password and the user box password.

  F.ADMIN verifies that the quality of the user box password is composed of ASCII code (0x20-0x7E, except 0x22 and 0x2B) in total of 93 characters by eight digits and is not composed of one kind of characters.

  F.BOX verifies that the quality of the user box password is composed of ASCII code (0x20-0x7E, except 0x22 and 0x2B) in total of 93 characters by eight digits and is not composed of one kind of characters.

  F.PRINT verifies that the quality of the secure print password is composed of ASCII code

(0x20-0x7E, except 0x22 and 0x2B) in total 93 characters by eight digits and is not composed of one kind of characters.
Accordingly, this functional requirement is satisfied.

- **FIA_SOS.1[5]**
  FIA_SOS.1[5] regulates the quality of the session information.
  F.ADMIN verifies that a space quality is more than 10^{10} as the quality of session information.
  F.BOX verifies that a space quality is more than 10^{10} as the quality of session information.
  Accordingly, this functional requirement is satisfied.

- **FIA_SOS.2**
  FIA_SOS.2 regulates the generation of session information and its quality.
  F.ADMIN generates the secrets that are the space quality of 10^{10} or more to session information in the administrator authentication.
  F.BOX generates the secrets that are the space quality of 10^{10} or more to session information in the user box authentication.
  Accordingly, this functional requirement is satisfied.

- **FIA_UAU.2[1]**
  FIA_UAU.2[1] regulates the authentication of the service engineer.
  F.SERVICE authenticates that the user who accesses the service mode by using the CE password is the service engineer.
  Accordingly, this functional requirement is satisfied.

- **FIA_UAU.2[2]**
  FIA_UAU.2[2] regulates the authentication of the administrator.
  F.ADMIN authenticates that the user who accesses the administrator mode by using the administrator password is the administrator.
  F.ADMIN-SNMP authenticates that the user who accesses the MIB object by using the SNMP password (Privacy password, Authentication password) is the administrator.
  Accordingly, this functional requirement is satisfied.

- **FIA_UAU.2[3]**
  FIA_UAU.2[3] regulates the authentication of the authorized user to use the secure print file.
  F.PRINT authenticates that the user is the authorized user to use the secure print file by using the secure print password that is set to each secure print file.
  Accordingly, this functional requirement is satisfied.

- **FIA_UAU.2[4]**
  FIA_UAU.2[4] regulates the authentication of the authorized user to use the user box.
  F.BOX authenticates that the user is the authorized user to use the user box by using the user box password that is set to each user box.
  Accordingly, this functional requirement is satisfied.

- **FIA_UAU.6**
  FIA_UAU.6 regulates the re-authentication for the important operation such as changing a password.

F.ADMIN re-authenticates the administrator at the operation for the change of the administrator password. Along with the change operation of the HDD lock password and encryption passphrase, by collating the registered HDD lock password and registered encryption passphrase, it re-authenticates the administrator who has known each of confidential information.

F.SERVICE re-authenticates the service engineer at the operation of the change of the CE password.

Accordingly, this functional requirement is satisfied.

- **FIA_UAU.7**

FIA_UAU.7 regulates the return of “*" as the feedback under the authentication.

F.ADMIN returns “*" for each character for entered administrator password from the panel in the authentication and re-authentication of administrator, and prevents a direct display of the administrator password.

F.SERVICE returns “*" for each character for the entered CE password from the panel in the authentication and re-authentication of the service engineer, and prevents a direct display of the CE password.

F.PRINT returns “*" for each character for the entered secure print password from the panel in the authentication of the authorized user who can use the secure print file, and prevents the direct display of the secure print password.

F.BOX returns "*" for each character for the entered user box password from the panel in the authentication of the user who is permitted the use of the public user box, and prevents a direct display of the user box password.

Accordingly, this functional requirement is satisfied.

- **FIA_UID.2[1]**

FIA_UID.2[1] regulates the identification of the service engineer.

F.SERVICE identifies the user who accesses the service mode is a service engineer.

Accordingly, this functional requirement is satisfied.

- **FIA_UID.2[2]**

FIA_UID.2[2] regulates the authentication of the administrator.

F.ADMIN identifies the user who accesses the administrator mode is an administrator.

F.ADMIN-SNMP identifies the user, who accesses the MIB object, is an administrator.

Accordingly, this functional requirement is satisfied.

- **FIA_UID.2[3]**

FIA_UID.2[3] regulates the identification of the user who is permitted the use of the secure print file.

F.PRINT identifies a user who is permitted the use of the secure print file by selecting the secure print file as an operation target.

Accordingly, this functional requirement is satisfied.

- **FIA_UID.2[4]**

FIA_UID.2[4] regulates the identification of the user who is permitted the use of the user box.

F.BOX identifies the user who is permitted the use of the user box by selecting the user box as the operation target.

Accordingly, this functional requirement is satisfied.

- **FIA_USB.1**

  FIA_USB.1 regulates the security attribute association to subject that substitutes the user.
  F.PRINT associates the "secure pint internal control ID" of the concerned secure print file to the task of substituting the user when authenticated for the access to the secure print file..
  F.BOX associates the "User Box ID" of the concerned user box to the task of substituting the user when authenticated for the access to the user box file.
  Accordingly, this functional requirement is satisfied.

- **FMT_MOF.1[1]**

  FMT_MOF.1[1] regulates the behavior management of the enhanced security function.
  F.ADMIN provides the settings of the enhanced security function in the administrator mode, and manages the stop operation of the concerned function. In addition, although it is possible to change the back-up data acquired by back-up operation and to set off the Enhanced Security function as a result of performing the restoration operation, F.ADMIN limits the back-up and restoration operation only to the administrator. Although the execution of the HDD logical format and the overwrite deletion function of all area makes the Enhanced Security setting invalid, F.ADMIN permits the operation only to the administrator.
  F.SERVICE offers the HDD logical format function, HDD physical format function, the HDD installation setting function and the initialization function to make the Enhanced Security function invalid in the service mode along with execution and manages the setting-off operation of the Enhanced Security function.
  Accordingly, this functional requirement is satisfied.

- **FMT_MOF.1[2]**

  FMT_MOF.1[2] regulates the behavior management of the SNMP password authentication.
  F.ADMIN permits the operation of setting function of SNMP password authentication function in the administrator mode.
  F.ADMIN-SNMP permits the administrator who is authenticated by the SNMP password the setting operation of the SNMP password authentication.
  Accordingly, this functional requirement is satisfied.

- **FMT_MOF.1[3]**

  FMT_MOF.1[3] regulates the behavior management of the setup function.
  F.SERVICE offers the operation setting function of setup function in service mode and manages the operation function of setup function.
  Accordingly, this functional requirement is satisfied.

- **FMT_MSA.3**

  FMT_MSA.3 regulates the secure print internal control ID that is set at the time of registration of secure print file.
  F_PRINT grants the secure print internal control ID that is identified uniquely to the concerned secure print file at the time of registration of secure print file.
  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[1]**

  FMT_MTD.1[1] regulates the management of a SNMP password, the failure number of times threshold, and a secure print password.

  F.ADMIN permits the operation to change the SNMP password and the setting data of authentication failure frequency threshold in the administrator mode. In addition, F.ADMIN permits the administrator the back-up and restoration operation, and so it is possible to change the back-up data which is acquired by back-up operation, and to change a SNMP password, the failure number of times threshold and a secure print password as a result of performing the restoration operation.

  F.SNMP-ADMIN permits the change of the SNMP password.

  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[2]**

  FMT_MTD.1[2] regulates the management of the user box password.

  F.ADMIN permits the change operation of the user box password that is set to the user box in the administrator mode. In addition, F.ADMIN permits the administrator the back-up and restoration operation, and so it is possible to change the back-up data which is acquired by back-up operation, and to change the user box password as a result of performing the restoration operation.

  F.BOX permits the change operation of the user box password to the authenticated user as the user who is permitted the use of the user box concerned.

  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[3]**

  FMT_MTD.1[3] regulates the management of the administrator password.

  F.ADMIN permits the change operation of the administrator password in the administrator mode.

  F.SERVICE permits the change operation of the administrator password in the service mode.

  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[4]**

  FMT_MTD.1[4] regulates the management of the SNMP password, the User box password and the Secure Print password.

  F.ADMIN permits the administrator the back-up and restoration operation, and so it is possible to browse the SNMP password, the User box password and the Secure Print password by means of the back-up data which is acquired by back-up operation.

  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[5]**

  FMT_MTD.1[5] regulates the management of the CE password.

  F.SERVICE permits the change operation of the CE password in the service mode.

  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[6]**

  FMT_MTD.1[6] regulates the management of the administrator password and the SNMP password.

F.ADMIN permits the initialization operation of the administrator password and the SNMP password, that is performed along with the execution of the overwrite deletion operation of all area in the administrator mode.

F.SERVICE permits the initialization operation of the administrator password and the SNMP password, which is performed along with the execution of the initializing function in the service mode.

Accordingly, this functional requirement is satisfied.

- **FMT_SMF.1**

FMT_SMF.1 specifies the security management function.

F.ADMIN provides the following security management functions.

- Setting function of authentication failure frequency threshold
- Back-up and restoration function

  It consequentially corresponds to the inquiry function of the following TSF data.
  - SNMP password
  - User box password
  - Secure Print password

  It also corresponds to the modification function of the following TSF data.
  - SNMP password
  - User box password
  - Secure print password
  - Operational setting data of the Enhanced Security function
  - Authentication failure frequency threshold of the authentication operation prohibited function
- Stop function of the Enhanced Security function
  - Operational setting function of the Enhanced Security function
  - HDD logical format function
- Modification function of the administrator password
- Modification function of the user box password
- Modification function of the SNMP password (Privacy password and Authentication password)
- Lock release function

  This offers the following authentication functions.
  - Authentication function in the access to the MIB object
  - Authentication function in the access to the user box
  - Authentication function in the access to the secure print

F.ADMIN-SNMP offers security management functions.

- Modification function of the SNMP password (Privacy password and Authentication password)
- Operational setting function of the SNMP password authentication function

F.SERVICE offers the following security management functions.

- Modification function of the CE password
- Modification function of the administrator password
- Operation setting function of setup function
- Initialization function of the administrator password
  - Initialization function
- Initialization function of the SNMP password (Privacy password and Authentication

password）

・Initialization function

- ➢ Stop function of the Enhanced Security function

  ・HDD logical format function

  ・HDD physical format function

  ・HDD installation setting function

  ・Initialization function

F.BOX offers the following security management functions.

- ➢ Modification function of the user box password

F.ADMIN offers the following security management functions.

- ➢ Stop function of the Enhanced Security function

  ・Overwrite deletion function of all area

- ➢ Initialization of the administrator password

  ・Overwrite deletion function of all area

- ➢ Initialization of the SNMP password (Privacy password and Authentication password）

  ・Overwrite deletion function of all area

Accordingly, this functional requirement is satisfied.

- **FMT_SMR.1[1]**

FMT_SMR.1[1] regulates the role as the service engineer.

F.SERVICE recognizes the user who is authenticated by the CE password as a service engineer.

Accordingly, this functional requirement is satisfied.

FMT_SMR.1[2]

FMT_SMR.1[2] regulates the role as an administrator.

F.ADMIN recognizes the user who is authenticated by the administrator password as an administrator.

F.ADMIN-SNMP recognizes the user who is authenticated by the SNMP password（Privacy password and Authentication password） as an administrator.

Accordingly, this functional requirement is satisfied.

- **FMT_SMR.1[3]**

FMT_SMR.1[3] regulates the role as a user who is permitted the use of the user box.

F.BOX recognizes the user who is authenticated by the user box password as the authorized user who can use the user box.

Accordingly, this functional requirement is satisfied.

- **FPT_RVM.1**

FPT_RVM.1 regulates to support that a corresponding TSP execution function must be called before each TOE security function is permitted to start its operation.

F.ADMIN definitely activates "Administrator authentication function" of which performance is indispensable, before the use of various functions that can be performed only by administrator is permitted.

F.ADMIN-SNMP definitely activates "Administrator authentication function" of which performance is indispensable, before the use of network functions that can be performed only by administrator is permitted.

F.SERVICE definitely activates "Service engineer authentication function" of which performance is indispensable, before the use of various functions that can be performed only by the service engineer is permitted.

F.BOX definitely activates "Authentication function by the user box password" of which performance is indispensable, before the use of various functions that can be performed only by the authorized user who can use the user box is permitted.

F.PRINT definitely activates "Authentication function by the secure print password" of which performance is indispensable, before the use of various functions that can be performed only by the authorized user who can use the secure print is permitted.

F.HDD definitely activates "Validity verification function of HDD" of which performance is indispensable, before writing HDD is permitted when HDD lock function is activated.

Accordingly, this functional requirement is satisfied.

- **FPT_SEP.1**

FPT_SEP.1 regulates maintaining of security domains for protecting against interference and tampering by subjects who cannot be trusted and regulates separating of security domains of subjects.

F.ADMIN maintains the administrator authentication domain that is provided various functions permitted to operate only by administrator, and it does not permit the interference by the unauthorized subject.

F.ADMIN-SNMP maintains the administrator authentication domain that is provided various functions permitted to operate only by the administrator who is authenticated with the SNMP password, and it doesn't permit the interference by the unauthorized subjects.

F.BOX maintains the user box authentication domain that is provided various functions permitted to operate only by the authorized user who can use the user box by the authentication of the user box password, and it doesn't allow the interference by the unauthorized subject.

F.PRINT maintains the secure print file authentication domain that is provided various functions permitted to operate only by a user who is permitted to use the secure print file by the authentication of the secure print password, and it doesn't allow the interference by the unauthorized subject.

F.SERVICE maintains the service engineer authentication domain that is provided various functions permitted to operate only by the service engineer, and it doesn't allow the interference by the unauthorized subject.

Accordingly, this functional requirement is satisfied.

- **FNEW_RIP.1**

FNEW_RIP.1 regulates that the object and the TSF data, that are targeted in the explicit deletion operation can not be restored.

F.OVERWRITE-ALL deletes the user box file, the secure print file, the on-memory image file, the stored image file, the remaining image file, the image related file, the user box password, the secure print password and the remaining TSF data by performing the overwrite deletion to all area of HDD by means of the specified method of overwrite deletion.

In addition, it initializes the NVRAM administrator password and the SNMP password, and sets OFF the operations of the HDD lock function and the Encryption function.

Accordingly, this functional requirement is satisfied.

- **FIA_NEW.1**
  FIA_NEW.1 regulates the user identification before TSF takes any action to the user.
  F.HDD provides the function to check the HDD status if HDD lock password is set, and if the HDD lock password is not set, it doesn't perform the process of writing and reading to HDD.
  Accordingly, this functional requirement is satisfied.

8.3.2. Rational for TOE Security Strength of Function

The TOE security functions having a probabilistic/permutational mechanism are as follows.

① Administrator authentication mechanism offered by F.ADMIN
② CE authentication mechanism offered by F.SERVICE
③ Secure print authentication mechanism offered by F.PRINT
④ User box authentication mechanism offered by F.BOX
⑤ SNMP authentication mechanism offered by F.ADMIN-SNMP
⑥ HDD Lock password collation mechanism offered by F.ADMIN
⑦ Encryption Passphrase collation mechanism offered by F.ADMIN

It used the password composed from ①&② an 8-digits and 92 kinds of character, ③&④ an 8-digits and 93 kinds of character, ⑤ an 8-digits and 95 kinds of character, and ⑥&⑦ an 20-digits and 83 kinds of character. Among these, ①～⑤ locks the authentication function by the continuous three times of authentication failure by operating the authentication operation prohibition function.

The ① and ④ use the session information secretly in access via network. The secrets use the value of 10^{10} or more that is generated by TOE. Moreover, it uses the session information with the value of 10^{10} or more that is given externally.

Accordingly, as claimed in Section 6.2, the strength of function of mechanisms adequately satisfies the SOF-Basis, and it is consistent with the minimum strength of function: SOF-Basic that is claimed for the TOE security functional requirement for the security strength of function, stipulated in item 5.1.2.

8.3.3. Mutually Supported TOE Security Functions

The TOE security functional requirements that are satisfied by a combination of IT security functions that are identifies in the TOE summary specifications, are as shown in the text regarding the rationale in the section of 8.3.1.

8.3.4. Rationale for Assurance Measures

The required document for the evaluation assurance level EAL3 is covered by the reference document shown in the assurance measures described in Section 6.4. The TOE security assurance requirements are satisfied through development, test condition, vulnerability analysis, the development environment control, configuration management, life cycle management, and delivery procedures in accordance with the document provided as the assurance measures, as well as the preparation of a proper guidance document.

8.4. PP calims rationale

There is no PP that is referenced by this ST.