



**KONICA MINOLTA**

*bizhub 500 / bizhub 420 / ineo 500 / ineo 420*

*Control Software*

*Security Target*

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

Version : 1.14

Issued on : February 13, 2007

Created by : KONICA MINOLTA BUSINESS TECHNOLOGIES, NC.

## &lt;Revision History&gt;

Date	Ver.	Division	Approved	Checked	Created	Revision
2005/09/12	1.00	Development Div. 11	Yamazaki	Kakutani	Oda	Initial Version
2006/07/13	1.01	Development Div. 11	Yamazaki	Kakutani	Oda	Correct specification change. <ul style="list-style-type: none"> <li>• Correct method of Secure print function</li> <li>• Correct backup function via. USB (Service Engineer)</li> <li>• Correct a description of hardware configuration</li> </ul>
2006/10/11	1.02	Development Div. 11	Yamazaki	Kakutani	Oda	Correct specification change. <ul style="list-style-type: none"> <li>• Recorrect method of Secure print function back to ver1.00</li> <li>• Delete backup function via. USB</li> <li>• Correct a description of maintenance function permission specification</li> </ul>
2006/10/20	1.03	Development Div. 11	Yamazaki	Kakutani	Oda	<ul style="list-style-type: none"> <li>• Add maintenance function permission specification to security requirement.</li> <li>• Change HDD processing</li> <li>• Correct description of basic function in 2.</li> </ul>
2006/10/24	1.04	Development Div. 11	Yamazaki	Kakutani	Oda	<ul style="list-style-type: none"> <li>• Revise TOE version</li> <li>• Delete a description of physical formatting (Specification Change)</li> <li>• Change a description of maintenance function</li> </ul>
2006/11/02	1.05	Development Div. 11	Yamazaki	Kakutani	Oda	<ul style="list-style-type: none"> <li>• Correct a description of security target according to the other machine's ST amendment</li> </ul>
2006/11/10	1.06	Development Div. 11	Yamazaki	Kakutani	Oda	<ul style="list-style-type: none"> <li>• Correct typos error in FMT_MOF.1[3]</li> <li>• Define clearly the description about kinds of maintenance functions</li> </ul>
2006/11/16	1.07	Development Div. 11	Yamazaki	Kakutani	Oda	<ul style="list-style-type: none"> <li>• Correct the expression about initializing function in service and Add the relation between it and security enforcement setting</li> <li>• Correct Typos</li> </ul>
2006/11/22	1.08	Development Div. 11	Yamazaki	Kakutani	Oda	<ul style="list-style-type: none"> <li>• Correct Typos</li> </ul>
2006/12/22	1.09	Development Div. 11	Yamazaki	Kakutani	Oda	<ul style="list-style-type: none"> <li>• Remove HDD lock password in data for backup restore</li> <li>• Change the explanation as HDD stored setting will be affected security enforcement setting. And remove it from functions for initialization.</li> </ul>
2006/12/25	1.10	Development Div. 11	Yamazaki	Kakutani	Oda	<ul style="list-style-type: none"> <li>• Correct the access control for setting management</li> </ul>
2006/03/01	1.11	Development Div. 11	Yamazaki	Kakutani	Oda	<ul style="list-style-type: none"> <li>• Correct typos, etc.</li> </ul>
2006/04/04	1.12	Development Div. 11	Yamazaki	Kakutani	Oda	<ul style="list-style-type: none"> <li>• Correct typos, etc.</li> </ul>
2006/06/14	1.13	Development Div. 11	Yamazaki	Kakutani	Oda	<ul style="list-style-type: none"> <li>• Correct typos</li> </ul>
2006/07/05	1.14	Development Div. 11	Yamazaki	Kakutani	Oda	<ul style="list-style-type: none"> <li>• Correct typos.</li> </ul>

## 【 Contents 】

<b>1. ST Introduction .....</b>	<b>5</b>
1.1. ST Identification .....	5
1.2. TOE Identification .....	5
1.3. CC Conformance Claim .....	5
1.4. ST Overview .....	6
<b>2. TOE Description .....</b>	<b>7</b>
2.1. TOE Type .....	7
2.2. Environment for the usage of MFP .....	7
2.3. Operation Environment of the TOE .....	8
2.4. Role of the TOE User .....	9
2.5. Functions provided by the TOE .....	10
2.5.1. Basic Function .....	10
2.5.2. User Box Function .....	11
2.5.3. User Authentication Function .....	11
2.5.4. Administrator Function .....	12
2.5.5. Service Engineer Function .....	13
2.5.6. Other Functions .....	14
2.5.7. Enhanced Security Function .....	14
<b>3. TOE Security Environment .....</b>	<b>16</b>
3.1. Concept of Protected Assets .....	16
3.2. Assumptions .....	17
3.3. Threats .....	17
3.4. Organizational Security Policies .....	19
<b>4. Security Objectives .....</b>	<b>20</b>
4.1. Security Objectives for the TOE .....	20
4.2. Security objectives for the environment .....	21
4.2.1. IT environment security objectives .....	21
4.2.2. Non-IT environment security objective .....	21
<b>5. IT Security Requirements .....</b>	<b>23</b>
5.1. TOE Security Requirements .....	23
5.1.1. TOE Security Function Requirements .....	23
5.1.2. Minimum Security Strength of Function .....	45
5.1.3. TOE Security Assurance Requirements .....	46
5.2. Security Requirements for the IT environment .....	46
<b>6. TOE Summary Specification .....</b>	<b>48</b>
6.1. TOE Security Functions .....	48
6.1.1. F.ADMIN (Administrator Function) .....	48
6.1.2. F.ADMIN-SNMP (SNMP administrator function) .....	54
6.1.3. F.SERVICE (Service mode function) .....	55
6.1.4. F.USER (User Function) .....	57
6.1.5. F.BOX (User Box Function) .....	58
6.1.6. F.PRINT (Secure Print Function) .....	60
6.1.7. F.OVERWRITE-ALL (All area overwrite deletion function) .....	61
6.1.8. F.CRYPT (Encryption key generation function) .....	62

6.1.9. F.HDD (HDD verification function) .....	62
6.1.10. F.RESET (Authentication Failure Frequency Reset Function) .....	63
6.2. TOE Security Strength of Function .....	63
6.3. Correspondence between TOE Security Functions and Function Requirements .....	63
6.4. Assurance Measures .....	63
<b>7. PP Claims .....</b>	<b>65</b>
<b>8. Rational .....</b>	<b>66</b>
8.1. Security Objectives Rationale .....	66
8.1.1. Necessity .....	66
8.1.2. Sufficiency of Assumptions .....	67
8.1.3. Sufficiency of Threats .....	68
8.1.4. Sufficiency of Organizational Security Policies .....	70
8.2. IT Security Requirements Rationale .....	70
8.2.1. Rationale for IT Security Functional Requirements .....	70
8.2.2. Rational for Minimum Strength of Function .....	92
8.2.3. Rationale for IT Security Assurance Requirements .....	92
8.2.4. Consistency rationale for the set of IT security functional requirement .....	92
8.3. Rational for TOE Summary Specifications .....	93
8.3.1. Rational for the TOE Security Functions .....	93
8.3.2. Rational for TOE Security Strength of Function .....	110
8.3.3. Mutually Supported TOE Security Functions .....	111
8.3.4. Rationale for Assurance Measures .....	111
8.4. PP calims rationale .....	111

## 【 List of Figures 】

Figure 1 An example of the expected environment for usage of the MFP .....	7
Figure 2 Hardware composition that relates to TOE .....	8

## 【 List of Tables 】

Table 1 Box Access Control Operational List .....	24
Table 2 Secure Print File Access Control Operational List .....	24
Table 3 Setting Management Access Control Operational List .....	25
Table 4 TOE Security Assurance Requirements .....	46
Table 5 List of security function name and identifier of TOE .....	48
Table 6 Character and number of digits used for password .....	49
Table 7 A type of overwrite deletion of all domains and a method of overwrite .....	52
Table 8 Correspondence between TOE Assurance Requirements and assurance measures .....	64
Table 9 Conformity of Security Objectives to assumptions and Threats .....	66
Table 10 Conformity of IT Security Functional Requirements to Security Objectives .....	70
Table 11 Dependencies of IT Security Functional Requirements Components .....	83
Table 12 Mutual Support Correlations of IT Security Functional Requirements .....	86
Table 13 Conformity of TOE Security Functions to TOE Security Functional Requirements .....	93

## 1. ST Introduction

### 1.1. ST Identification

- ST Title : bizhub 500 / bizhub 420 / ineo 500 / ineo 420 Control Software Security Target
- ST Version : 1.14
- CC Version : 2.1、CCIMB Interpretations-0407
- Created on : February 13, 2007
- Created by : KONICA MINOLTA BUSINESS TECHNOLOGIES, INC. Akihko Oda

### 1.2. TOE Identification

- TOE Name : Japan :  
bizhub 500 / bizhub 420 / ineo 500 / ineo 420 Zentai Seigy Software  
Overseas :  
bizhub 500 / bizhub 420 / ineo 500 / ineo 420 Control Software
- TOE Version : 50GA-0100-G00-21-000
- 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  
CC Version 2.1, Part2 Extended
- Security assurance requirement  
CC Version2.1, Part3 Conformant
- Evaluation assurance level  
EAL3 Conformant (No additional assurance component)
- PP Reference  
This ST does not carry out a PP reference.
- Complement  
Apply CCIMB Interpretations-0407.

- Reference
  - Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031
  - Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032
  - Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033
  - CCIMB Interpretations-0407
  - Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model Version 2.1 August 1999 CCIMB-99-031 (January 2001 Translation Version 1.2, Information-technology Promotion Agency Japan, Security Center )
  - Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements Version 2.1 August 1999 CCIMB-99-032 (January 2001 Translation Version 1.2, Information-technology Promotion Agency Japan, Security Center )
  - Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements Version 2.1 August 1999 CCIMB-99-033 (January 2001 Translation Version 1.2, Information-technology Promotion Agency Japan, Security Center )
  - CCIMB Interpretations - 0210 Version 2<sup>1</sup> (August 2004 Information-technology Promotion Agency Japan, Security Center, Information Security Certification Office )
  - CCIMB Interpretations - 0407 ( August 2004 Information-technology Promotion Agency Japan, Security Center, Information Security Certification Office )

#### 1.4. ST Overview

bizhub 500, bizhub 420, ineo 500, ineo 420 is Konica Minolta Business Technologies, Inc. digital MFP comprised by selecting and combining copy, print, scan and FAX functions. ( Hereafter, “MFP” as all these generic names ) . The target of evaluation (TOE) of this Security Target (ST) is the “bizhub 500, bizhub 420, ineo 500, ineo 420,” that controls the entire operation of MFP, including the operation control processing and the image data management that are accepting from the panel of the main body of MFP 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 MFP. Moreover, TOE can encrypt all data including the image data written in HDD for the danger of taking HDD that is the medium that stores the image data in MFP out illegally by installing the encryption board which is the option parts of MFP. 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 MFP 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.

---

<sup>1</sup> Translation of CCIMB Interpretations- 0407 is shown in supplementation 0407 and 0210 in the 2nd edition.

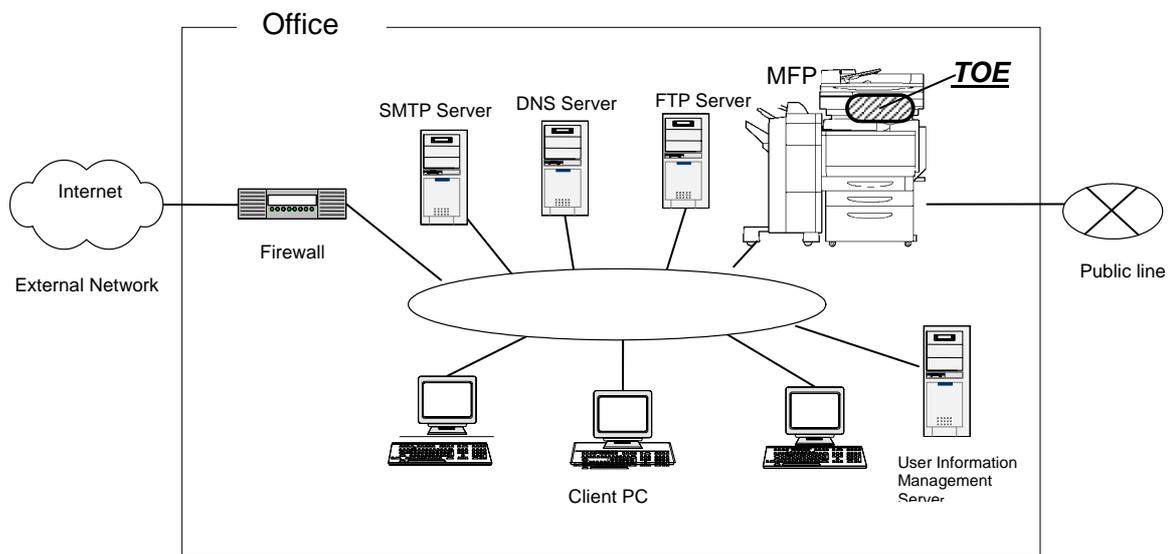
## 2. TOE Description

### 2.1. TOE Type

The bizhub 500/bizhub 420/ineo 500/ineo 420 Control Software that is the TOE is an embedded software product that controls the operation of whole MFP overall in the flash memory on the MFP controller.

### 2.2. Environment for the usage of MFP

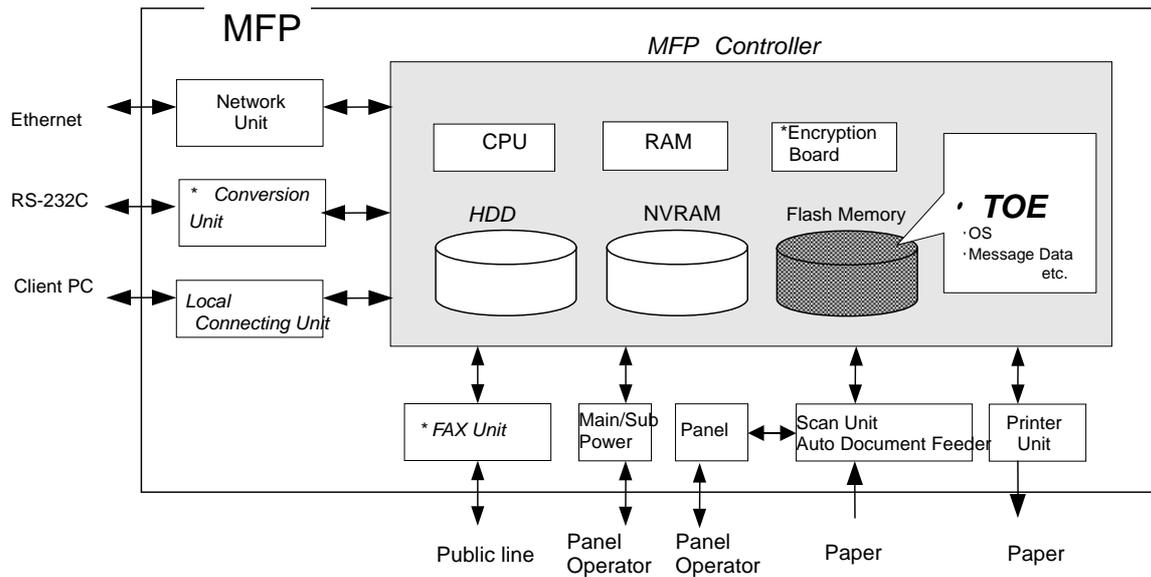
Figure 1 shows the expected general environment for the usage of MFP equipped with TOE. Moreover, the matters, assumed in the environment for the usage, show by a run of the item below.



**Figure 1 An example of the expected environment for usage of the MFP**

- The intra-office LAN exists as a network in the office.
- The MFP connects to the client PCs via the intra-office LAN, and has mutual data communication.
- When the SMTP server or FTP server are connected to the intra-office LAN, the MFP can carry out data communication with these. (Need the DNS Service when setting the Domain name of SMTP Server or FTP Server )
- The case, which is unifying management of the user ID and the user password in the server, also assumes. In this case, TOE can control the access to the MFP by using the user registration information in the user information management server.
- When the intra-office LAN connects to an external network, measures such as connecting via a firewall are taken, and an appropriate setup to block access requests to the MFP from the external network is 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.
- The public line connected with MFP is used to communicate with the FAX and the remote support function.

## 2.3. Operation Environment of the TOE



**Figure 2 Hardware composition that relates to TOE**

Figure 2 shows the structure of the hardware environment on the MFP that TOE needs for the operation. TOE exists on the flash memory on the MFP controller which builds in the body of the MFP and is loaded and run on the RAM.

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

- Flash memory

Storage medium that stores the object code of the “MFP 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

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 MFP used for processing of TOE.

- Encryption Board ( \* An 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 MFP as standard for convenience' sake of a sale, but is sold as an optional part.

- Panel

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

- Main power supply

The power switch for activating MFP

- Network Unit

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

- Local Connecting Unit

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 MFP.

- Conversion Unit ( \* Option parts )

A unit for connection with RS232C through serial port. When breaking down, the maintenance function can be used through this.

- FAX Unit ( \* Option parts )

A device that is used for the communication for sending and receiving FAX and for the remote diagnosis function (described later) via public line. According to the circumstances in sales, it is sold as the option part and is not attached on the MFP.

- Scan Unit / An automatic manuscript feeder

The device that scans images and photos from a paper and converts them into the digital data.

- Printer Unit

The device that actually prints the converted image data for printing when demanded to print by the MFP controller.

- 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 MFP with the TOE are defined as follows.

- User  
MFP's user who is registered into MFP. ( In general, the employee in the office is assumed. )
  
- Administrator  
MFP's user who carries out the management of the operation of MFP. An administrator performs the operation management of MFP and the management of user. (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 MFP. Service Engineer performs the repair and adjustment of MFP. (In general, the person in charge at the sales companies that performs the maintenance service of MFP and is in cooperation with Konica Minolta Business Technologies Inc. is assumed.)
  
- Person in charge at the Organization that uses the MFP  
A person in charge at the organization that manages the office where the MFP is installed. This person assigns an administrator who carries out the management of the operation of the MFP.
  
- Person in charge at the Organization that manages the Maintenance of the MFP  
A person in charge at the organization that carries out management of the maintenance for the MFP. This person assigns service engineers who perform the maintenance management for the MFP.

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 user's awareness.

### 2.5.1. Basic Function

In MFP, a series of function for the office work concerning the image such as copy, print, scan, and fax exists as a basic function, and TOE performs the core control in the operation of these functions. It converts the raw data acquired from the external device of the MFP controller into the image file, and registered in RAM and HDD. (After two or more conversion processing is done, the conversion is done as for the print image file from PC.) The image file is converted to data for the print or for the transmission, and is transmitted to the device outside of the MFP controller concerned.

Operations of copy, print, scan, and fax are managed by the unit of job, and can be changed the

operation order, can be modified the finishing if it's a printing 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 data 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. Two types of user box exist; one is the personal user box which a user possesses and the other is the public user box which the registered user making a group within a certain number uses jointly. As for the personal user box, the operation is limited only for the user who owns it and the public user box performs access control by sharing a password set to the user box among users.

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, transmission, and download from client PC, of image file in a user box
- Deletion of the image file in the user box, and move and copy to other user boxes
- Storage period setting of image file in user box (Delete automatically after the period passes.)
- Change of user box name, change of the password, and deletion of user box, etc.
- Attribute setting of user box (classification change of a personal user box or a public user box)

### **2.5.3. User Authentication Function**

TOE can limit the user who uses MFP. When accessing it through the panel or the network, TOE performs the identification and authentication that the user is permitted to use the MFP by applying the user password and user ID. When the identification and authentication succeeds, TOE permits the user the use of the basic function and the user box function, etc.

Several types of the following are supported in the method of the user authentication.

#### Machine authentication

A method to authenticate on MFP by registering a user ID and a user password into HDD on MFP controller.

#### External server authentication

A method to authenticate with processing the authentication on MFP by using the user ID and the user password that are registered on the user information management server which is connected by the intra-office LAN without managing the user ID and user

password on the MFP side. Though two or more methods named Active Directory<sup>2</sup>, NTLM<sup>3</sup>, and NDS are supported, the method of the external server authentication assumed in this ST is applied only the case with Active Directory.

#### 2.5.4. Administrator Function

TOE provides the functions such as the management of user boxes, management of user information at the time of MPF authentication 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.

- The user registration management at machine authentication
  - Registration or change in user ID and user password, and deletion of a user.
- Management of user box settings
  - Registration or change in user box password, and management of user attributes
- Operation setting of automatic system reset
  - Setting of the function that logs out automatically when the setting time passed.
- Management of network setting
  - Connection setting of the intra-office LAN (setting of DNS server)
  - SMTP setting (setting of SMTP server utilized by E-mail transmission)
  - IP address, NetBIOS name and AppleTalk printer name etc.
- Backup or 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.
- Modification function of administrator password

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

- Method setting of a user authentication function
  - Select the machine authentication, the external server authentication, or the user authentication stop.
- User: Setting of access by PUBLIC
  - Select the permission and prohibition of MFP utilization of the user who is not identified by user ID.
- Setting of a password policy function

---

<sup>2</sup> A method of directory service that Windows Server 2000 (after it) offers to consolidate user information in network environment of Windows platform.

<sup>3</sup> Abbreviation of NT LAN Administrator. Authentic method used in directory service that Windows NT offers to consolidate user information in network environment of Windows platform.

- 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.

### 2.5.5. Service Engineer Function

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

- Modification function of administrator password
- Modification function of CE<sup>4</sup> password

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

- Authentication setting of the service engineer with the CE password.
  - Select ON or OFF.
- 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.

---

<sup>4</sup>Abbreviation of Customer Service engineer

- Setting of maintenance function (through serial port or through LAN)
  - 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. 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.

### Encryption key generation function

When the encryption board, an optional product, is installed in MFP 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.

### 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 MFP, the access to HDD is permitted by the matching of the HDD lock password set to the HDD and the one set on the MFP. (Even if HDD is taken out, it is impossible to use it excluding the MFP that the concerned HDD installed.)

### Remote diagnostic function

Making use of several connected systems such as E-mail, and a modem connection through a FAX public line mouth or a RS-232C, in communication with support center of MFP produced by Konica Minolta business technologies Ltd., it manages the state condition of MFP 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.

### 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.

## 2.5.7. Enhanced Security Function

Various setting functions related to the behavior of the security function for the Administrator function and the Service engineer function can be set collectively to the secure values by the operation settings of the “Enhanced Security Function”. Each value set is prohibited changing itself into the vulnerable one individually. As the function that does not have a setting function of the operation individually, 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 user identification and authentication function : Valid ( Either the machine authentication, or the external server authentication are available )
- User : Setting of access of PUBLIC : Prohibit
- Setting of a service engineer authentication function : Valid
- 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 (via serial port)
- Remote diagnostic function : Prohibit
- Network setting management reset function : Prohibit
- TOE update function via Internet : Prohibit
- Modification function of administrator password via http : Prohibit
- Installation setting function of HDD : 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 MFP is generally used, the following image file in available situation becomes the protected assets.

- 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 MFP or mail server is connected by any chance, the setting of MFP (IP address etc.) requires not to be modified illegally. Therefore, the setting of MFP (IP address etc.) is considered as subsidiary protected assets.

On the other hand, when the stored data have physically been separated from the jurisdiction of a user, such as the use of MFP 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
- Transmission Address Data File
  - File including E-mail address and telephone numbers that become the destination to transmit an image.

## 3.2. Assumptions

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

### **A.ADMIN ( Personnel conditions to be an administrator )**

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

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

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

### **A.NETWORK ( Network connection conditions for MFP )**

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

### **A.SECRET ( Operational condition about secret information )**

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

### **A.SETTING ( MFP Operational setting condition like Enhanced Security function )**

- After Enhanced Security function is set valid, MFP with the TOE will be used.
- After maintenance function (through LAN) is set prohibited, MFP with the TOE will be used.

### **A.SERVER( Management condition of the user information management server connected to the intra-office LAN )**

When the external server authentication is used for the user authentication method, the user information management server that is connected with the intra-official LAN installing MFP with TOE are performed appropriately the management of the account, access control and patch application, etc.

## 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-MFP ( Lease-return and disposal of MFP )**

When the leaser returned or the discarded MFP 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, the transmission address data file, and the set various passwords can leak by the person with malicious intent taking out and analyzing an HDD in MFP.

### **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, a transmission address data file, and the set-up various passwords can leak by a person or a user with malicious intent illegally taking out and analyzing an HDD in MFP.

- A person or a user with malicious intent illegally replaces an HDD in MFP. 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, a transmission address data 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-PRIVATE-BOX ( Unauthorized access to the personal user box which used a user function )**

Exposure of the user box file when a person or a user with malicious intent accesses the user box where other user owns, and downloads, prints and transmits the user box file (E-mail transmission, FTP transmission, fax transmission, and SMB<sup>5</sup> transmission).

#### **T.ACCESS-PUBLIC-BOX ( Unauthorized access to public box which used a user function )**

Exposure of the user box file when a person or the user with malicious intent accesses the public user box which is not permitted to use, and downloads, prints, transmits (E-mail transmission, FTP transmission, FAX transmission and SMB transmission) and removes and copies to the other user box the 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 settings that is related to the transmission of a user box file. Even an addressee is set precisely, a user box file is transmitted (the E-mail transmission or the FTP transmission) to the entity which a user does not intend to, so that a user box file is exposed.
  - < The network setting which is related to user box file transmission >
    - Setting related to the SMTP server
    - Setting related to the DNS server
- Malicious person or user changes the network setting which set in MFP to identify MFP itself where TOE installed, by setting to the value of the entity such as another illegal MFP from the value of MFP (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 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 )**

---

<sup>5</sup>Abbreviation of Server Message Block. Protocol to realize the file sharing or printer sharing on Windows.

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.REGISTERED-USER ( Utilization of registered user )**

TOE permits only the registered user to use the MFP installing TOE.

#### **O.PRIVATE-BOX ( Personal user box access control )**

- TOE permits only a user to use the user function of the personal user box which this user owns.
- TOE permits only a user to use the user function of the use box file in the personal user box which this user owns.

#### **O.PUBLIC-BOX ( Public user box access control )**

- TOE permits the registered user the reading operation of the public user box.
- TOE permits the user functions of the public user box only to the user who is permitted the use of this public user box.
- TOE permits the user functions of the user box file in the public user box only to the user who is permitted the use of this public 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 SMTP server
- The setting function related to the DNS server
- The setting function related to the address of MFP
- Backup function
- Restoration function

TOE permits the operation 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 MFP by using the deletion of data, and makes all the image data restoration impossible. In addition, TOE offers a function to initialize a setting value such as the highly confidential password that is set by a user or an administrator.

**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 MFP.

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

TOE verifies that 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 MFP encrypts all data including an image file to be written in HDD inside MFP and then stores it to an HDD.

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

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

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

The application of a browser etc. used by client PC to access MFP offers the appropriate feedback protected for input user password, 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 MFP will assign a person who can faithfully execute the given role during the operation of the MFP 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 MFP 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 the MFP with TOE.
- The administrator observes the maintenance work of MFP with TOE by a service engineer.

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

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

intercept the access from an external network to MFP with TOE.

#### **OE-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 user password, secure print password and the user box password.
- The user password and the user box password should be properly changed.
- When the administrator changes the user password or 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.SERVER ( Secure user information management server )**

The person in charge in the organization who uses MFP manages the user information management server secure to the user information management server such as account management, application of the patch done, and execution of the access control appropriately made.

#### **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 like Enhanced Security function )**

- The administrator makes the enhanced security function effective for the operation of TOE.
- The service engineer should set maintenance function(through LAN) prohibit 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

<b>FCS_CKM.1</b>		<b>Cryptographic key generation</b>	
FCS_CKM.1.1			
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: <i>cryptographic key generation algorithm</i> ] and specified cryptographic key sizes [assignment: <i>cryptographic key sizes</i> ] that meet the following: [assignment: <i>list of standards</i> ].			
[assignment: <i>list of standards</i> ] :			
<b><i>KonicaMinolta Encryption specification standard</i></b>			
[assignment: <i>cryptographic key generation algorithm</i> ] :			
<b><i>KonicaMinolta HDD Encryption key generation algorithm (SHA-1)</i></b>			
[assignment: <i>cryptographic key sizes</i> ] :			
<b><i>128bit</i></b>			
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

<b>FDP_ACC.1[1]</b>	<b>Subset access control</b>
FDP_ACC.1.1[1]	
The TSF shall enforce the [assignment: <i>access control SFP</i> ] on [assignment: <i>list of subjects, objects, and operations among subjects and objects covered by the SFP</i> ].	
[assignment: <i>list of subjects, objects, and operations among subjects and objects covered by the SFP</i> ] : <b>Listed in Table1 User Box Access Control: Operational List</b>	
[assignment: <i>access control SFP</i> ] : <b>User Box access control</b>	
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
<i>A task to act for a user</i>	<i>User Box</i>	<ul style="list-style-type: none"> <li>• <i>A List of user boxes</i></li> </ul>
	<i>User Box File</i>	<ul style="list-style-type: none"> <li>• <i>Print</i></li> <li>• <i>Transmission (E-mail transmission, FTP transmission, SMB transmission and FAX transmission)</i></li> <li>• <i>Download</i></li> <li>• <i>Move to other user boxes</i></li> <li>• <i>Copy to other user boxes</i></li> <li>• <i>Backup</i></li> </ul>

<b>FDP_ACC.1[2]</b>	<b>Subset access control</b>
FDP_ACC.1.1[2]	
The TSF shall enforce the [assignment: <i>access control SFP</i> ] on [assignment: <i>list of subjects, objects, and operations among subjects and objects covered by the SFP</i> ].	
[assignment: <i>list of subjects, objects, and operations among subjects and objects covered by the SFP</i> ] : <b>Listed in Tabel2 Secure Print File Access Control: Operational List</b>	
[assignment: <i>access control SFP</i> ] : <b>Secure print file access control</b>	
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
<i>A task to act for a user</i>	<i>Secure Print File Access Control</i>	<ul style="list-style-type: none"> <li>• <i>A List of Secure Print Files</i></li> <li>• <i>Print</i></li> <li>• <i>Back-Up</i></li> </ul>

<b>FDP_ACC.1[3]</b>	<b>Subset access control</b>
FDP_ACC.1.1[3]	
The TSF shall enforce the [assignment: <i>access control SFP</i> ] on [assignment: <i>list of subjects, objects, and operations among subjects and objects covered by the SFP</i> ].	
[assignment: <i>list of subjects, objects, and operations among subjects and objects covered by the SFP</i> ] : <b>Listed in Table 3 Setting Management Access Control: Operational List</b>	
[assignment: <i>access control SFP</i> ] : <b>Setting management access control</b>	

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
<i>A task to act for a user</i>	• <i>HDD Lock Password Object</i>	• <i>Settings</i>
	• <i>Encryption passphrase Object</i>	• <i>Settings</i> • <i>Back-Up</i> • <i>Restore</i>
	• <i>SMTP Server Group Object</i> • <i>DNS Server Group Object</i> • <i>MFP Address Group Object</i> <sup>6</sup>	• <i>Settings</i> • <i>Restore</i>

<b>FDP_ACF.1[1]</b>	<b>Security attribute based access control</b>
FDP_ACF.1.1[1]	
The TSF shall enforce the [assignment: <i>access control SFP</i> ] to objects based on the following: [assignment: <i>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</i> ].	
[assignment: <i>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</i> ] :	
<p>&lt; <i>Subject</i> &gt;</p> <ul style="list-style-type: none"> <li>• <i>A task to act for a user</i></li> </ul>	<p>&lt; <i>Subject attributes</i> &gt;</p> <ul style="list-style-type: none"> <li>• <i>User Attribute ( User ID )</i></li> <li>• <i>User Box Attribute ( User Box ID )</i></li> <li>• <i>Administrator Attribute</i></li> </ul>
-----	
<p>&lt; <i>Object</i> &gt;</p> <ul style="list-style-type: none"> <li>• <i>User Box</i></li>   <li>• <i>User Box File</i></li> </ul>	<p>&lt; <i>Object attributes</i> &gt;</p> <ul style="list-style-type: none"> <li>• <i>User Attribute ( User ID or Public )</i></li>   <li>• <i>User Attribute ( User ID or Public )</i></li> <li>• <i>User Box Attribute ( User Box ID )</i></li> </ul>
[assignment: <i>access control SFP</i> ] :	
<b><i>User Box access control</i></b>	
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: <i>rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects</i> ].	
[assignment: <i>rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects</i> ] :	
<p>&lt; <i>Operation control to Personal user box</i> &gt;</p> <p><i>A task to act for a user is permitted to do the list display operation to the user box with the user attribute (user ID) of an object attribute corresponding to the user attribute (user ID) of the subject attribute.</i></p>	
<p>&lt; <i>Operation control to user box file in Personal user box</i> &gt;</p> <p><i>A task to act for a user is permitted to print, transmit (E-mail transmission, FTP transmission, SMB transmission and FAX transmission), download, move to other user boxes and copy to the other user boxes, to the user box file that have the matched user attributes (User ID) and user box attribute (user box ID) of the object attribute with the user attributes (User ID) and user box attribute (user box ID) of the subject attribute.</i></p>	
<p>&lt; <i>Operation control to Public user box</i> &gt;</p>	

<sup>6</sup>The MFP address group object is a series of data concerning the address of the main body of MFP such as IP address and the Appletalk printer name.

<p><i>A task to act for the user who is related to the user attribute (user ID) is permitted to do the list display operation to the user box where "Public" is set to the user attributes of the object attribute.</i></p> <p><b>&lt; Operation control to a user box file in Public user box &gt;</b>  <i>A task to act for the user who is related to the user attribute (User ID) and user box attribute (user box ID) is permitted to print, transmit (E-mail transmission, FTP transmission, SMB transmission, and fax transmission), download, move to other user boxes, and copy operation to other user boxes to the user box file that "Public" is set to the user attribute of the object attribute and has matched user box attribute with the user box attribute of subject attribute.</i></p>	
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] :	
<ul style="list-style-type: none"> <li>• <i>A task to act for the user that has an administrator attribute is permitted to operate displaying of user box list.</i></li> <li>• <i>A task to act for the user that has an administrator attribute is permitted to operate the back-up the user box file.</i></li> </ul>	
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] :	
<b>None</b>	
Hierarchical to	: No other components
Dependencies	: FDP_ACC.1 ( FDP_ACC.1[1] ) FMT_MSA.3 ( FMT_MSA.3[1] )

<b>FDP_ACF.1[2] Security attribute based access control</b>	
FDP_ACF.1.1[2]	
The TSF shall enforce the [assignment: <i>access control SFP</i> ] to objects based on the following: [assignment: <i>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</i> ].	
[assignment: <i>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</i> ] :	
<p><b>&lt; Subject &gt;</b></p> <ul style="list-style-type: none"> <li>• <i>task substituted for a user</i></li> </ul>	<p><b>&lt; Subject attributes &gt;</b></p> <ul style="list-style-type: none"> <li>• <i>File attributes ( Secure print internal control ID )</i></li> <li>• <i>User attributes ( User ID )</i></li> <li>• <i>Administrator attributes</i></li> </ul>
-----	
<p><b>&lt; Object &gt;</b></p> <ul style="list-style-type: none"> <li>• <i>Secure print file</i></li> </ul>	<p><b>&lt; Object attributes &gt;</b></p> <ul style="list-style-type: none"> <li>• <i>File attributes ( Secure print internal control ID )</i></li> </ul>
[assignment: <i>access control SFP</i> ] :	
<b>Secure print file access control</b>	
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: <i>rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects</i> ].	
[assignment: <i>rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects</i> ] :	
<ul style="list-style-type: none"> <li>• <i>A task to act for a user who has a user attribute (user ID) is permitted to display of the list of all the secure print files.</i></li> <li>• <i>A task to act for a user who has a user attribute (user ID) and the 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).</i></li> </ul>	
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] :	

<b><i>A task to act for a user who has an administrator attribute is permitted to back up secure print file.</i></b>	
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] : <b>None</b>	
Hierarchical to	: No other components
Dependencies	: FDP_ACC.1 ( FDP_ACC.1[2] ) FMT_MSA.3 ( FMT_MSA.3[2] )

<b>FDP_ACF.1[3] Security attribute based access control</b>	
FDP_ACF.1.1[3]	
The TSF shall enforce the [assignment: <i>access control SFP</i> ] to objects based on the following: [assignment: <i>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</i> ].	
[assignment: <i>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</i> ] :	
<b>&lt; Subject &gt;</b> <ul style="list-style-type: none"> <li>• <i>Task substituted for a user</i></li> </ul>	<b>&lt; Subject attributes &gt;</b> <ul style="list-style-type: none"> <li>• <i>Administrator attributes</i></li> <li>• <i>CE attributes</i></li> </ul>
-----	
<b>&lt; Object &gt;</b> <ul style="list-style-type: none"> <li>• <i>HDD Lock Password Object</i></li> <li>• <i>Encryption passphrase object</i></li> <li>• <i>SMTP server group object</i></li> <li>• <i>DNS server group object</i></li> <li>• <i>MFP address group object</i></li> </ul>	
[assignment: <i>access control SFP</i> ] : <b>Setting management access control</b>	
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: <i>rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects</i> ].	
[assignment: <i>rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects</i> ] :	
<ul style="list-style-type: none"> <li>• <i>A task 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.</i></li> <li>• <i>A task for a user who has an administrator attribute is permitted to backup the encryption passphrase object, and to operate the restoration.</i></li> <li>• <i>A task for a user who has an administrator attribute is permitted to set the SMTP server group object, the DNS server group object and the MFP address group object, and to operate the restoration.</i></li> <li>• <i>A task for a user who has a CE attribute is permitted to set the HDD lock password object and the encryption passphrase object.</i></li> </ul>	
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] : <b>None</b>	
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] : <b>None</b>	
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: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] unsuccessful authentication attempts occur related to <i>[assignment: list of authentication events]</i> .	
<i>[assignment: list of authentication events]</i> : <ul style="list-style-type: none"> <li>• <b>Authentication for accessing the service mode</b></li> <li>• <b>Re-authentication for changing the CE password.</b></li> </ul>	
[selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] <b><i>[assignment: range of acceptable values]</i> : an administrator configurable positive integer within 1 ~ 3</b>	
FIA_AFL.1.2[1]	
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall <i>[assignment: list of actions]</i> .	
<i>[assignment: list of actions]</i> : <p>&lt; <b>Action when it is detected</b> &gt;</p> <ul style="list-style-type: none"> <li>• <b>Log off from the authentication status of the service mode if it is, and lock the authentication function which uses the CE password.</b></li> <li>• <b>If it's not under the authentication status, lock the authentication function which uses the CE password.</b></li> </ul> <p>&lt; <b>Operation for recovering the normal condition</b> &gt;  <b>Perform the boot process of the TOE.</b></p>	
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: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] unsuccessful authentication attempts occur related to <i>[assignment: list of authentication events]</i> .	
<i>[assignment: list of authentication events]</i> : <ul style="list-style-type: none"> <li>• <b>Authentication for accessing the administrator mode</b></li> <li>• <b>Re-authentication for changing the administrator password</b></li> </ul>	
[selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] <b><i>[assignment: range of acceptable values]</i> : an administrator configurable positive integer within 1 ~ 3</b>	
FIA_AFL.1.2[2]	
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall <i>[assignment: list of actions]</i> .	
<i>[assignment: list of actions]</i> : <p>&lt; <b>Action when it is detected</b> &gt;</p> <ul style="list-style-type: none"> <li>• <b>Log off from the authentication status of the administrator mode if it is, and lock the authentication function which uses the administrator password.</b></li> <li>• <b>If it's not under the authentication status, lock the authentication function which uses the administrator password.</b></li> </ul> <p>&lt; <b>Operation for recovering the normal condition</b> &gt;  <b>Perform the boot process of the TOE.</b></p>	
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: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i> ].	
[assignment: <i>list of authentication events</i> ] :	
<b><i>Authentication for accessing the MIB object through SNMP</i></b>	
[selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ]	
<b><i>[assignment: range of acceptable values] : an administrator configurable positive integer within 1 ~ 3</i></b>	
FIA_AFL.1.2[3]	
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: <i>list of actions</i> ].	
[assignment: <i>list of actions</i> ] :	
<b>&lt;Action when it is detected &gt;</b>	
<b><i>Deny the access to the MIB object and lock the authentication function to use SNMP password.</i></b>	
<b>&lt;Operation for recovering the normal condition &gt;</b>	
<ul style="list-style-type: none"> <li>• <b><i>Perform the lock release function offered within the administrator mode.</i></b></li> <li>• <b><i>Reboot the TOE.</i></b></li> </ul>	
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: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i> ].	
[assignment: <i>list of authentication events</i> ] :	
<b><i>Authentication for accessing the TOE by user</i></b>	
[selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ]	
<b><i>[assignment: range of acceptable values] : an administrator configurable positive integer within 1 ~ 3</i></b>	
FIA_AFL.1.2[4]	
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: <i>list of actions</i> ].	
[assignment: <i>list of actions</i> ] :	
<b>&lt;Action when it is detected &gt;</b>	
<b><i>Log off from the authentication status of the user if it is, and lock the authentication function for the user.</i></b>	
<b>&lt;Operation for recovering the normal condition &gt;</b>	
<ul style="list-style-type: none"> <li>• <b><i>Perform the lock release function offered within the administrator mode.</i></b></li> <li>• <b><i>Reboot the TOE.</i></b></li> </ul>	
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: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i> ].	
[assignment: <i>list of authentication events</i> ] :	

<b>Authentication for accessing the secure print file</b>	
[selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> <b><i>[assignment: range of acceptable values] : an administrator configurable positive integer within 1 ~ 3</i></b>	
FIA_AFL.1.2[5]	
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall <i>[assignment: list of actions]</i> .	
<i>[assignment: list of actions] :</i> <b>&lt; Action when it is detected &gt;</b> <i>Deny the access to the secure print file and lock the authentication function for the secure print file.</i> <b>&lt; Operation for recovering the normal condition &gt;</b> <ul style="list-style-type: none"> <li>• <i>Perform the lock release function offered within the administrator mode.</i></li> <li>• <i>Reboot the TOE.</i></li> </ul>	
Hierarchical to	: No other components
Dependencies	: FIA_UAU.1 ( FIA_UAU.2[4] )

<b>FIA_AFL.1[6] Authentication failure handling</b>	
FIA_AFL.1.1[6]	
The TSF shall detect when [selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] unsuccessful authentication attempts occur related to <i>[assignment: list of authentication events]</i> .	
<i>[assignment: list of authentication events]</i> . : <b>Authentication for accessing the public user box</b>	
[selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> <b><i>[assignment: range of acceptable values] : an administrator configurable positive integer within 1 ~ 3</i></b>	
FIA_AFL.1.2[6]	
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall <i>[assignment: list of actions]</i> .	
<i>[assignment: list of actions] :</i> <b>&lt; Action when it is detected &gt;</b> <i>Log off from the authentication status of the user box if it is, and lock the authentication function for the concerned user box.</i> <b>&lt; Operation for recovering the normal condition &gt;</b> <ul style="list-style-type: none"> <li>• <i>Perform the lock release function offered within the administrator mode.</i></li> <li>• <i>Reboot the TOE.</i></li> </ul>	
Hierarchical to	: No other components
Dependencies	: FIA_UAU.1 ( FIA_UAU.2[5] )

<b>FIA_AFL.1[7] Authentication failure handling</b>	
FIA_AFL.1.1[7]	
The TSF shall detect when [selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> ] unsuccessful authentication attempts occur related to <i>[assignment: list of authentication events]</i> .	
<i>[assignment: list of authentication events]</i> : <ul style="list-style-type: none"> <li>• <i>Authentication when it accesses service mode</i></li> <li>• <i>Authentication when it accesses administrator mode from the panel</i></li> <li>• <i>Authentication when user accesses TOE from the panel</i></li> <li>• <i>Authentication when it accesses secure print file</i></li> <li>• <i>Authentication when it accesses Public user box from the panel</i></li> </ul>	
[selection: <i>[assignment: positive integer number]</i> , an administrator configurable positive integer within <i>[assignment: range of acceptable values]</i> <b><i>[assignment: positive integer number] : 1</i></b>	

FIA_AFL.1.2[7]	
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: <i>list of actions</i> ].	
[assignment: <i>list of actions</i> ] : <b>&lt;Action when it is detected &gt;</b> <i>Deny all access from the panel.</i> <b>&lt;Operation for recovering the normal condition &gt;</b> <ul style="list-style-type: none"> <li>• <i>Automatically release the lock after 5 seconds.</i></li> </ul>	
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_UAU.2[5] )

<b>FIA_ATD.1                      User attribute definition</b>	
FIA_ATD.1.1	
The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: <i>list of security attributes</i> ].	
[assignment: <i>list of security attributes</i> ] : <ul style="list-style-type: none"> <li>• <i>User box attributes ( User box ID )</i></li> <li>• <i>File attributes ( Secure print internal control ID )</i></li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_SOS.1[1]                      Verification of secrets</b>	
FIA_SOS.1.1[1]	
The TSF shall provide a mechanism to verify that <u>secrets</u> ( <i>Administrator Password, CE Password</i> ) meet [assignment: <i>a defined quality metric</i> ].	
[assignment: <i>a defined quality metric</i> ] : <ul style="list-style-type: none"> <li>• <i>Number of digits: 8- digits</i></li> <li>• <i>Character type: ASCII code ( 0x21 ~ 0x7E, except 0x22 and 0x2B )</i></li> <li>• <i>Rule : Do not composed by only the same kind of character strings.</i>  <i>Do not set the same password as the current setting.</i></li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_SOS.1[2]                      Verification of secrets</b>	
FIA_SOS.1.1[2]	
The TSF shall provide a mechanism to verify that <u>secrets</u> ( <i>SNMP Password</i> ) meet [assignment: <i>a defined quality metric</i> ].	
[assignment: <i>a defined quality metric</i> ] : <ul style="list-style-type: none"> <li>• <i>Number of digits: 8- digits</i></li> <li>• <i>Character type: ASCII code 0x20 ~ 0x7E)</i></li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_SOS.1[3]                      Verification of secrets</b>	
FIA_SOS.1.1[3]	
The TSF shall provide a mechanism to verify that <u>secrets</u> ( <i>User Password</i> ) meet [assignment: <i>a defined</i>	

<i>quality metric</i> ].	
[assignment: <i>a defined quality metric</i> ] :	
<ul style="list-style-type: none"> <li>• <b>Number of digits: 8- digits</b></li> <li>• <b>Character type: ASCII code ( 0x21 ~ 0x7E, except 0x22 and 0x2B )</b></li> <li>• <b>Rule : Do not composed by only the same kind of character strings.</b></li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_SOS.1[4]</b>	<b>Verification of secrets</b>
FIA_SOS.1.1[4]	
The TSF shall provide a mechanism to verify that <u>secrets</u> ( <b><i>HDD Lock Password, Encryption passphrase</i></b> ) meet [assignment: <i>a defined quality metric</i> ].	
[assignment: <i>a defined quality metric</i> ] :	
<ul style="list-style-type: none"> <li>• <b>Number of digits: 20- digits</b></li> <li>• <b>Character type: ASCII code ( 0x21 ~ 0x7E, except 0x22, 0x28, 0x29, 0x2C, 0x3A, 0x3B, 0x3C, 0x3E, 0x5B, 0x5C and 0x5D )</b></li> <li>• <b>Rule : Do not composed by only the same kind of character strings. Do not set the same password or passphrase as the current setting.</b></li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_SOS.1[5]</b>	<b>Verification of secrets</b>
FIA_SOS.1.1[5]	
The TSF shall provide a mechanism to verify that <u>secrets</u> ( <b><i>Secure print password, User box password</i></b> ) meet [assignment: <i>a defined quality metric</i> ].	
[assignment: <i>a defined quality metric</i> ] :	
<ul style="list-style-type: none"> <li>• <b>Number of digits: 8- digits</b></li> <li>• <b>Character type: ASCII code ( 0x20 ~ 0x7E, except 0x22 and 0x2B )</b></li> <li>• <b>Rule : Do not composed by only the same kind of character strings.</b></li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_SOS.1[6]</b>	<b>Verification of secrets</b>
FIA_SOS.1.1[6]	
The TSF shall provide a mechanism to verify that <u>secrets</u> ( <b><i>Session Information</i></b> ) meet [assignment: <i>a defined quality metric</i> ].	
[assignment: <i>a defined quality metric</i> ] :	
<b><i>10<sup>10</sup> and above</i></b>	
Hierarchical to	: No other components
Dependencies	: No dependencies

<b>FIA_SOS.2</b>	<b>TSF Generation of secrets</b>
FIA_SOS.2.1	
The TSF shall provide a mechanism to generate secrets ( <b><i>Session information</i></b> ) that meet [assignment: <i>a defined quality metric</i> ].	
[assignment: <i>a defined quality metric</i> ] :	
<b><i>10<sup>10</sup> and above</i></b>	

FIA_SOS.2.2	
The TSF shall be able to enforce the use of TSF generated secrets for [assignment: <i>list of TSF functions</i> ].	
[assignment: <i>list of TSF functions</i> ] :	
<ul style="list-style-type: none"> <li>• <b>Administrator authentication (Access through the network)</b></li> <li>• <b>User authentication (Access through the network)</b></li> <li>• <b>User box authentication (Access through the network)</b></li> </ul>	
Hierarchical to	: No other components
Dependencies	: No dependencies

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

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

<b>FIA_UAU.2[3]                      User authentication before any action</b>	
FIA_UAU.2.1[3]	
The TSF shall require each <u>user</u> ( <b><i>User</i></b> ) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <b><i>User</i></b> ).	
Hierarchical to	: FIA_UAU.1
Dependencies	: FIA_UID.1 ( FIA_UID.2[3] )

<b>FIA_UAU.2[4]                      User authentication before any action</b>	
FIA_UAU.2.1[4]	
The TSF shall require each <u>user</u> ( <b><i>User who is permitted to use secure print file</i></b> ) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <b><i>User who is permitted to use secure print file</i></b> ).	
Hierarchical to	: FIA_UAU.1
Dependencies	: FIA_UID.1 ( FIA_UID.2[4] )

<b>FIA_UAU.2[5]                      User authentication before any action</b>	
FIA_UAU.2.1[5]	
The TSF shall require each <u>user</u> ( <b><i>User who is permitted to use the public user box</i></b> ) to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <b><i>User who is permitted to use the public user box</i></b> ).	

Hierarchical to	:	FIA_UAU.1
Dependencies	:	FIA_UID.1 ( FIA_UID.2[5] )

<b>FIA_UAU.6</b>		<b>Re-authenticating</b>
FIA_UAU.6.1		
The TSF shall re-authenticate the use under the conditions [assignment: <i>list of conditions under which re-authentication is required</i> ].		
[assignment: <i>list of conditions under which re-authentication is required</i> ]		
<ul style="list-style-type: none"> <li>• <b><i>When the administrator modifies the administrator password.</i></b></li> <li>• <b><i>When the service engineer modifies the CE password.</i></b></li> <li>• <b><i>When the administrator changes the HDD lock setting.</i></b></li> <li>• <b><i>When the administrator changes the Encryption function setting.</i></b></li> </ul>		
Hierarchical to	:	No other components
Dependencies	:	No dependencies

<b>FIA_UAU.7</b>		<b>Protected authentication feedback</b>
FIA_UAU.7.1		
The TSF shall provide only [assignment: <i>list of feedback</i> ] to the user while the authentication is in progress.		
[assignment: <i>list of feedback</i> ] :		
<b><i>Display "*" every character data input.</i></b>		
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_UAU.2[5] )

<b>FIA_UID.2[1]</b>		<b>User identification before any action</b>
FIA_UID.2.1[1]		
The TSF shall require each <u>user</u> ( <i>Service Engineer</i> ) to identify itself before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>Service Engineer</i> ).		
Hierarchical to	:	FIA_UID.1
Dependencies	:	No dependencies

<b>FIA_UID.2[2]</b>		<b>User identification before any action</b>
FIA_UID.2.1[2]		
The TSF shall require each <u>user</u> ( <i>Administrator</i> ) to identify itself before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>Administrator</i> ).		
Hierarchical to	:	FIA_UID.1
Dependencies	:	No dependencies

<b>FIA_UID.2[3]</b>		<b>User identification before any action</b>
FIA_UID.2.1[3]		
The TSF shall require each <u>user</u> ( <i>User</i> ) to identify itself before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>User</i> ).		
Hierarchical to	:	FIA_UID.1

Dependencies	: No dependencies
--------------	-------------------

<b>FIA_UID.2[4]</b>	<b>User identification before any action</b>
FIA_UID.2.1[4]	
The TSF shall require each <u>user</u> ( <i>User who is permitted to use secure print file</i> ) to identify itself before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>User who is permitted to use secure print file</i> ).	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

<b>FIA_UID.2[5]</b>	<b>User identification before any action</b>
FIA_UID.2.1[5]	
The TSF shall require each <u>user</u> ( <i>User who is permitted to use the public user box</i> ) to identify itself before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>User who is permitted to use the public user box</i> ).	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

<b>FIA_UID.2[6]</b>	<b>User identification before any action</b>
FIA_UID.2.1[6]	
The TSF shall require each <u>user</u> ( <i>External server</i> ) to identify itself before allowing any other TSF-mediated actions on behalf of that <u>user</u> ( <i>External server</i> ).	
Hierarchical to	: FIA_UID.1
Dependencies	: No dependencies

<b>FIA_USB.1</b>	<b>User-subject binding</b>
FIA_USB.1.1	
The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.	
Hierarchical to	: No other components
Dependencies	: FIA_ATD.1

5.1.1.4. Security management

<b>FMT_MOF.1[1]</b>	<b>Management of security functions behaviour</b>
FMT_MOF.1.1[1]	
The TSF shall restrict the ability to [selection: <i>determine the behaviour of, disable, enable, modify the behaviour of</i> ] the functions [assignment: <i>list of functions</i> ] to [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>list of functions</i> ]	: • <b>Enhanced Security Setting</b>
[selection: <i>determine the behaviour of, disable, enable, modify the behaviour of</i> ]	: <b>disable</b>
[assignment: <i>the authorised identified roles</i> ]	:

	<ul style="list-style-type: none"> <li>• <b>Administrator</b></li> <li>• <b>Service Engineer</b></li> </ul>
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 ( FMT_SMF.1 ) FMT_SMR.1 ( FMT_SMR.1[1]、FMT_SMR.1[2] )

<b>FMT_MOF.1[2] Management of security functions behaviour</b>	
FMT_MOF.1.1[2]	
The TSF shall restrict the ability to [selection: <i>determine the behaviour of, disable, enable, modify the behaviour of</i> ] the functions [assignment: <i>list of functions</i> ] to [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>list of functions</i> ] :	
<ul style="list-style-type: none"> <li>• <b>User Authentication Function</b></li> <li>• <b>SNMP password authentication function</b></li> </ul>	
[selection: <i>determine the behaviour of, disable, enable, modify the behaviour of</i> ] :	
<b>modify the behaviour of</b>	
[assignment: <i>the authorised identified roles</i> ] :	
<b>Administrator</b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 ( FMT_SMF.1 ) FMT_SMR.1 ( FMT_SMR.1[2] )

<b>FMT_MOF.1[3] Management of security functions behaviour</b>	
FMT_MOF.1.1[3]	
The TSF shall restrict the ability to [selection: <i>determine the behaviour of, disable, enable, modify the behaviour of</i> ] the functions [assignment: <i>list of functions</i> ] to [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>list of functions</i> ] :	
<ul style="list-style-type: none"> <li>• <b>Maintenance Function (through LAN)</b></li> </ul>	
[selection: <i>determine the behaviour of, disable, enable, modify the behaviour of</i> ] :	
<b>enable</b>	
[assignment: <i>the authorised identified roles</i> ] :	
<b>Service Engineer</b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 ( FMT_SMF.1 ) FMT_SMR.1 ( FMT_SMR.1[1] )

<b>FMT_MSA.1[1] Management of security attributes</b>	
FMT_MSA.1.1[1]	
The TSF shall enforce the [assignment: <i>access control SFP, information flow control SFP</i> ] to restrict the ability to [selection: <i>change_default, query, modify, delete, [assignment: other operations]</i> ] the security attributes [assignment: <i>list of security attributes</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of security attributes</i> ] :	
<b>User attributes of the user box that is set user's own [user ID].</b>	
[selection: <i>change_default, query, modify, delete, [assignment: other operations]</i> ] :	
<b>modify ( modify to [public], or modify to other user's [User ID] )</b>	
[assignment: <i>the authorized identified roles</i> ] :	
<ul style="list-style-type: none"> <li>• <b>User</b></li> <li>• <b>Administrator</b></li> </ul>	
[assignment: <i>access control SFP, information flow control SFP</i> ] :	
<b>User box access control</b>	
Hierarchical to	: No other components
Dependencies	: FDP_ACC.1 or FDP_IFC.1 ( FDP_ACC.1[1] ) FMT_SMF.1 ( FMT_SMF.1 )

FMT\_SMR.1 ( FMT\_SMR.1[2]、 FMT\_SMR.1[3] )

<b>FMT_MSA.1[2] Management of security attributes</b>	
FMT_MSA.1.1[2]	
The TSF shall enforce the [assignment: <i>access control SFP, information flow control SFP</i> ] to restrict the ability to [selection: <i>change_default, query, modify, delete, [assignment: other operations]</i> ] the security attributes [assignment: <i>list of security attributes</i> ] to [assignment: <i>the authorized identified roles</i> ].	
[assignment: <i>list of security attributes</i> ] :	
<b>User attributes of user box that is set the [public].</b>	
[selection: <i>change_default, query, modify, delete, [assignment: other operations]</i> ] :	
<b>modify ( modify to [User ID] )</b>	
[assignment: <i>the authorized identified roles</i> ] :	
<ul style="list-style-type: none"> <li>• <b>User who is permitted to use that user box</b></li> <li>• <b>Administrator</b></li> </ul>	
[assignment: <i>access control SFP, information flow control SFP</i> ] :	
<b>User box access control</b>	
Hierarchical to	: No other components
Dependencies	: FDP_ACC.1 or FDP_IFC.1 ( FDP_ACC.1[1] ) FMT_SMF.1 ( FMT_SMF.1 ) FMT_SMR.1 ( FMT_SMR.1[2]、 FMT_SMR.1[4] )

<b>FMT_MSA.3[1] Static attribute initialization</b>	
FMT_MSA.3.1[1]	
The TSF shall enforce the [assignment: <i>access control SFP, information flow control SFP</i> ] to provide [selection, choose one of: <i>restrictive, permissive, [assignment: other property]</i> ] default values for security attributes ( <b>User attributes of the user box</b> ) that are used to enforce the SFP.	
[selection, choose one of: <i>restrictive, permissive, [assignment: other property]</i> ] :	
<b>[assignment: other property] :</b>	
<b>Responded the registered situation of the user box classified into the following cases.</b>	
<b>[Public], when an user box is registered by the operation of user or administrator</b>	
<b>[User ID] of the user who performed the relevant job, when an user box is registered automatically according to the operation of stored job specifying unregistered user box.</b>	
[assignment: <i>access control SFP, information flow control SFP</i> ] :	
<b>User box access control</b>	
FMT_MSA.3.2[1]	
The TSF shall allow the [assignment: <i>the authorized identified roles</i> ] to specify alternative initial values to override the default values when an object or information is created.	
[assignment: <i>the authorized identified roles</i> ]	
Case identified in [assignment: other property] of FMT_MSA.3.1	: User
Case identified in [assignment: other property] of FMT_MSA.3.1	: None
Hierarchical to	: No other components
Dependencies	: FMT_MSA.1 ( FMT_MSA.1[1]、 FMT_MSA.1[2] ) FMT_SMR.1 ( FMT_SMR.1[3] )

<b>FMT_MSA.3[2] Static attribute initialization</b>	
FMT_MSA.3.1[2]	
The TSF shall enforce the [assignment: <i>access control SFP, information flow control SFP</i> ] to provide [selection, choose one of: <i>restrictive, permissive, [assignment: other property]</i> ] default values for security attributes ( <b>Secure print internal control ID</b> ) that are used to enforce the SFP.	
[selection, choose one of: <i>restrictive, permissive, [assignment: other property]</i> ] :	
<b>[assignment: other property] : Identified uniquely</b>	
[assignment: <i>access control SFP, information flow control SFP</i> ] :	

<b><i>Secure print file access control</i></b>	
FMT_MSA.3.2[2]	
The TSF shall allow the [assignment: <i>the authorized identified roles</i> ] to specify alternative initial values to override the default values when an object or information is created.	
[assignment: <i>the authorized identified roles</i> ] <b><i>None</i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_MSA.1 ( N/A ) FMT_SMR.1 ( N/A )

<b>FMT_MTD.1[1] Management of TSF data</b>	
FMT_MTD.1.1[1]	
<b><i>( When the [machine authentication] is selected as the User authentication method )</i></b> The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] : <b><i>User password</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] : <b>[assignment: <i>other operations</i>] : <i>Registration</i></b>	
[assignment: <i>the authorised identified roles</i> ] : <b><i>Administrator</i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 ( FMT_SMF.1 ) FMT_SMR.1 ( FMT_SMR.1[2] )

<b>FMT_MTD.1[2] Management of TSF data</b>	
FMT_MTD.1.1[2]	
<b><i>( When the [machine authentication] is selected as the User authentication method )</i></b> The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] : <b><i>User's own user password</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] : <b><i>modify</i></b>	
[assignment: <i>the authorised identified roles</i> ] : • <b><i>User</i></b> • <b><i>Administrator</i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 ( FMT_SMF.1 ) FMT_SMR.1 ( FMT_SMR.1[2]、 FMT_SMR.1[3] )

<b>FMT_MTD.1[3] Management of TSF data</b>	
FMT_MTD.1.1[3]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] : • <b><i>User ID</i></b> • <b><i>SNMP password</i></b> • <b><i>Secure print password</i></b> • <b><i>Panel auto log-off time</i></b> • <b><i>Threshold Number of authentication failure</i></b> • <b><i>External server authentication setting data</i></b>	

[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] : <b><i>modify</i></b>
[assignment: <i>the authorised identified roles</i> ] : <b><i>Administrator</i></b>
Hierarchical to : No other components
Dependencies : FMT_SMF.1 ( FMT_SMF.1 ) 、 FMT_SMR.1 ( FMT_SMR.1[2] )

<b>FMT_MTD.1[4] Management of TSF data</b>	
FMT_MTD.1.1[4]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] : <b><i>User box password of the relevant user box</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] : <b><i>modify</i></b>	
[assignment: <i>the authorised identified roles</i> ] : <ul style="list-style-type: none"> <li>• <b><i>User who is permitted to use that public user box</i></b></li> <li>• <b><i>Administrator</i></b></li> </ul>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 ( FMT_SMF.1 ) \ FMT_SMR.1 ( FMT_SMR.1[2]、FMT_SMR.1[4] )

<b>FMT_MTD.1[5] Management of TSF data</b>	
FMT_MTD.1.1[5]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] : <b><i>User box password</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] : <b><i>[assignment: other operations] : Registration</i></b>	
[assignment: <i>the authorised identified roles</i> ] : <ul style="list-style-type: none"> <li>• <b><i>User</i></b></li> <li>• <b><i>Administrator</i></b></li> </ul>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 ( FMT_SMF.1 ) 、 FMT_SMR.1 ( FMT_SMR.1[2]、FMT_SMR.1[3] )

<b>FMT_MTD.1[6] Management of TSF data</b>	
FMT_MTD.1.1[6]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] : <ul style="list-style-type: none"> <li>• <b><i>Administrator password</i></b></li> </ul>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] : <b><i>modify</i></b>	
[assignment: <i>the authorised identified roles</i> ] : <ul style="list-style-type: none"> <li>• <b><i>Administrator</i></b></li> <li>• <b><i>Service Engineer</i></b></li> </ul>	
Hierarchical to	: No other components

Dependencies	:	FMT_SMF.1 ( FMT_SMF.1 ) , FMT_SMR.1 ( FMT_SMR.1[1]、 FMT_SMR.1[2] )
--------------	---	--

<b>FMT_MTD.1[7] Management of TSF data</b>		
FMT_MTD.1.1[7]		
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorised identified roles</i> ].		
[assignment: <i>list of TSF data</i> ] :		
<ul style="list-style-type: none"> <li>• <b><i>SNMP password</i></b></li> <li>• <b><i>User password</i></b></li> <li>• <b><i>User box password</i></b></li> <li>• <b><i>Secure print password</i></b></li> </ul>		
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :		
<b><i>query</i></b>		
[assignment: <i>the authorised identified roles</i> ] :		
• <b><i>Administrator</i></b>		
Hierarchical to	:	No other components
Dependencies	:	FMT_SMF.1 ( FMT_SMF.1 ) 、 FMT_SMR.1 ( FMT_SMR.1[2] )

<b>FMT_MTD.1[8] Management of TSF data</b>		
FMT_MTD.1.1[8]		
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorised identified roles</i> ].		
[assignment: <i>list of TSF data</i> ] :		
<b><i>Secure print password</i></b>		
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :		
<b><i>[assignment: other operations] : Registration</i></b>		
[assignment: <i>the authorised identified roles</i> ] :		
<b><i>User</i></b>		
Hierarchical to	:	No other components
Dependencies	:	FMT_SMF.1 ( FMT_SMF.1 ) 、 FMT_SMR.1 ( FMT_SMR.1[3] )

<b>FMT_MTD.1[9] Management of TSF data</b>		
FMT_MTD.1.1[9]		
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorised identified roles</i> ].		
[assignment: <i>list of TSF data</i> ] :		
<b><i>CE password</i></b>		
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :		
<b><i>modify</i></b>		
[assignment: <i>the authorised identified roles</i> ] :		
<b><i>Service Engineer</i></b>		
Hierarchical to	:	No other components
Dependencies	:	FMT_SMF.1 ( FMT_SMF.1 ) 、 FMT_SMR.1 ( FMT_SMR.1[1] )

<b>FMT_MTD.1[10] Management of TSF data</b>	
FMT_MTD.1.1[10]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] :	
<b><i>User ID</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :	
<b><i>[assignment: other operations] : Registration</i></b>	
[assignment: <i>the authorised identified roles</i> ] :	
<b><i>Administrator, External server</i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 ( FMT_SMF.1 ) 、 FMT_SMR.1 ( FMT_SMR.1[2]、 FMT_SMR.1[5] )

<b>FMT_MTD.1[11] Management of TSF data</b>	
FMT_MTD.1.1[11]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] :	
<b><i>SNMP password</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :	
<b><i>[assignment: other operations] : Initialization</i></b>	
[assignment: <i>the authorised identified roles</i> ] :	
<b><i>Administrator, Service Engineer</i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 ( FMT_SMF.1 ) 、 FMT_SMR.1 ( FMT_SMR.1[1]、 FMT_SMR.1[2] )

<b>FMT_MTD.1[12] Management of TSF data</b>	
FMT_MTD.1.1[12]	
The TSF shall restrict the ability to [selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] the [assignment: <i>list of TSF data</i> ] to [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>list of TSF data</i> ] :	
<b><i>Administrator password</i></b>	
[selection: <i>change_default, query, modify, delete, clear</i> , [assignment: <i>other operations</i> ]] :	
<b><i>[assignment: other operations] : Initialization</i></b>	
[assignment: <i>the authorised identified roles</i> ] :	
<b><i>Administrator</i></b>	
Hierarchical to	: No other components
Dependencies	: FMT_SMF.1 ( FMT_SMF.1 ) 、 FMT_SMR.1 ( FMT_SMR.1[1]、 FMT_SMR.1[2] )

<b>FMT_SME.1 Specification of Management Functions</b>	
FMT_SME.1.1	
The TSF shall be capable of performing the following security management functions: [assignment: <i>list of security management functions to be provided by the TSF</i> ].	
[assignment: <i>list of security management functions to be provided by the TSF</i> ] :	
<ul style="list-style-type: none"> <li>• <b><i>Stop Function of Enhanced security function by administrator</i></b></li> <li>• <b><i>Operation Method Setting Function of User Authentication Function by administrator</i></b></li> <li>• <b><i>Operation Setting Function of SNMP password authentication function by administrator</i></b></li> <li>• <b><i>Setting function of authentication failure frequency threshold by administrator in the</i></b></li> </ul>	

<p><i>authentication operation prohibition function</i></p> <ul style="list-style-type: none"> <li>• <i>Backup Function by administrator</i> <sup>7</sup></li> <li>• <i>Restoration Function by administrator</i> <sup>8</sup></li> <li>• <i>Panel Auto Log-off Time Setting Function by administrator</i></li> <li>• <i>Deletion Function of detected value of unauthorized access to SNMP by administrator</i></li> <li>• <i>Deletion Function of detected value of unauthorized access of user by administrator</i></li> <li>• <i>Deletion function of detected value of unauthorized access to secure print by administrator</i></li> <li>• <i>Deletion function of detected value of unauthorized access to user box by administrator</i></li> <li>• <i>Modification function of administrator password by administrator</i></li> <li>• <i>Modification function of SNMP password by administrator</i></li> <li>• <i>Modification function of user password by administrator</i></li> <li>• <i>Registration function of user box password by administrator</i></li> <li>• <i>Modification function of user box password by administrator</i></li> <li>• <i>User box registration function by administrator (However, only when the [public] is registered for user attribute.)</i></li> <li>• <i>Modification function of user attribute of the user box by the administrator (However, only when the user attribute of previous setting is "user ID")</i></li> <li>• <i>Registration function of user ID by administrator</i></li> <li>• <i>Registration function of user password when method of user authentication by administrator is machine authentication</i></li> <li>• <i>Modification function of user password when method of user authentication by administrator is machine authentication</i></li> <li>• <i>Initialization function of administrator password by administrator</i></li> <li>• <i>Initialization function of SNMP password by administrator</i></li> <li>• <i>Modification function of service engineer password by service engineer</i></li> <li>• <i>Modification function of administrator password by service engineer</i></li> <li>• <i>Stop function of Enhanced Security function by service engineer</i></li> <li>• <i>Activation function of maintenance function (through LAN) by service engineer</i></li> <li>• <i>Initialization function of SNMP password by service engineer</i></li> <li>• <i>Overwrite function for the default value of the user attribute of the user box by the user.</i></li> <li>• <i>Modification function of user password when method of user authentication is machine authentication by user</i></li> <li>• <i>Registration function of user box password by user</i></li> <li>• <i>Modification function of user attribute of user box by user</i></li> <li>• <i>User box registration function by user</i></li> <li>• <i>Automatic Personal user box registration function by user box stored job that specifies unregistered box by user</i></li> <li>• <i>Machine non-registered users' user ID automatic registration function with external server when user authentication method is external server authentication</i></li> <li>• <i>Registration function of secure print password according to secure print file registration by user</i></li> <li>• <i>Modification function of user attribute of user box by user who is permitted the use of public user box</i></li> <li>• <i>Modification function of user box password of the user box by user who is permitted the use of public user box</i></li> </ul>	
Hierarchical to	: <u>No other components</u>
Dependencies	: <u>No dependencies</u>

<b>FMT_SMR.1[1]</b>	<b>Security roles</b>
FMT_SMR.1.1[1]	The TSF shall maintain the roles [assignment: <i>the authorised identified roles</i> ].
	[assignment: <i>the authorised identified roles</i> ] : <b><i>Service Engineer</i></b>
FMT_SMR.1.2[1]	

<sup>7</sup> A part of a backup function corresponds to the inquiry function of TSF data.

<sup>8</sup> A part of the restoration function corresponds to the modification function of the TSF data.

The TSF shall be able to associate users with roles.	
Hierarchical to	: No other components
Dependencies	: FIA_UID.1 ( FIA_UID.2[1] )

<b>FMT_SMR.1[2] Security roles</b>	
FMT_SMR.1.1[2]	
The TSF shall maintain the roles [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>the authorised identified roles</i> ] :	
<b><i>Administrator</i></b>	
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] )

<b>FMT_SMR.1[3] Security roles</b>	
FMT_SMR.1.1[3]	
The TSF shall maintain the roles [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>the authorised identified roles</i> ] :	
<b><i>User</i></b>	
FMT_SMR.1.2[3]	
The TSF shall be able to associate users with roles.	
Hierarchical to	: No other components
Dependencies	: FIA_UID.1 ( FIA_UID.2[3] )

<b>FMT_SMR.1[4] Security roles</b>	
FMT_SMR.1.1[4]	
The TSF shall maintain the roles [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>the authorised identified roles</i> ] :	
<b><i>User who is authorized to use that public user box</i></b>	
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[5] )

<b>FMT_SMR.1[5] Security roles</b>	
FMT_SMR.1.1[5]	
The TSF shall maintain the roles [assignment: <i>the authorised identified roles</i> ].	
[assignment: <i>the authorised identified roles</i> ] :	
<b><i>External server</i></b>	
FMT_SMR.1.2[5]	
The TSF shall be able to associate users with roles.	
Hierarchical to	: No other components
Dependencies	: FIA_UID.1 ( FIA_UID.2[6] )

5.1.1.5. Protection of the TSF

<b>FPT_RVM.1</b>	<b>Non-bypassability of the TSP</b>
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

<b>FPT_SEP.1</b>	<b>TSF domain separation</b>
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. TOE Access

<b>FTA_SSL.3</b>	<b>TSF-initiated termination</b>
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [assignment: <i>time interval of user inactivity</i> ]. [assignment: <i>time interval of user inactivity</i> ] : <b><i>Time decided from the final operation depending on the panel auto logoff time (1-9 minute/s) while an administrator or a user is operating on the panel</i></b>
Hierarchical to	: No other components
Dependencies	: No dependencies

5.1.1.7. Extended requirement: Identification and approval of access destination

<b>FIA_NEW.1</b>	<b>Identification and approval of a user becoming an access object from TOE</b>
FIA_NEW.1.1	TSF shall demand to succeed in the user's identification before the action is taken to <u>user</u> ( <b>HDD</b> ) by TOE.
FIA_NEW.1.2	TSF shall stop the start of the action to <u>user</u> ( <b>HDD</b> ) 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 identification

information
Management : FIA_NEW.1
The following actions could be considered for the management functions in FMT. a) management of user identification information

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

<b>FNEW_RIP.1</b>	<b>Protection of remaining information on the user data and TSF data after explicit deletion operation</b>
FNEW_RIP.1.1	<p>TSF shall guarantee not to be able to use the content of any information before having been assigned to the resource on the explicit deleting operation to the following objects and the TSF data: [assignment: <i>list of object and list of TSF data</i>].</p> <p>[assignment : <i>List of object and list of TSF data</i>] :</p> <ul style="list-style-type: none"> <li>• <i>User Box file</i></li> <li>• <i>Secure print file</i></li> <li>• <i>On memory image file</i></li> <li>• <i>Stored image file</i></li> <li>• <i>Remaining image file</i></li> <li>• <i>Image-related file</i></li> <li>• <i>Transmission addressee data file</i></li> <li>• <i>HDD lock password object</i></li> <li>• <i>Encryption passphrase object</i></li> <li>&lt; <i>TSF data</i> &gt;</li> <li>• <i>Administrator password</i></li> <li>• <i>SNMP password</i></li> <li>• <i>User ID</i></li> <li>• <i>User password</i></li> <li>• <i>User Box password</i></li> <li>• <i>Secure print password</i></li> <li>• <i>Remaining TSF data</i><sup>9</sup></li> </ul> <p>Hierarchical to : No other components Dependencies : No dependencies</p>

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.2[5], FIA\_UAU.6, FIA\_SOS.1[1], FIA\_SOS.1[2], FIA\_SOS.1[3], FIA\_SOS.1[4], FIA\_SOS.1[5], FIA\_SOS.1[6] 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.

<sup>9</sup> TSF data remaining in the HDD data area, that cannot be deleted only by the deletion of the file management area.

### 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

<b>FCS_COP.1[E]</b>		<b>Cryptographic operation</b>
FCS_COP.1.1[E]		
The TSE( <i>Encryption board</i> ) shall perform [assignment: <i>list of cryptographic operations</i> ] in accordance with a specified cryptographic algorithm [assignment: <i>cryptographic algorithm</i> ] and cryptographic key sizes [assignment: <i>cryptographic key sizes</i> ] that meet the following: [assignment: <i>list of standards</i> ].		
[assignment: <i>list of standards</i> ] :		
<b>FIPS PUB 197</b>		
[assignment: <i>cryptographic algorithm</i> ] :		
<b>AES</b>		
[assignment: <i>cryptographic key sizes</i> ] :		
<b>128bit</b>		
[assignment: <i>list of cryptographic operations</i> ] :		
<ul style="list-style-type: none"> <li>• <b>Encryption of all data written in HDD</b></li> <li>• <b>Decryption of all data read from HDD</b></li> </ul>		
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

<b>FIA_AFL.1[E]</b>	<b>Authentication failure handling</b>
FIA_AFL.1.1[E]	
The <b>TSF (HDD)</b> shall detect when [selection: <i>assignment: positive integer number</i> ], an administrator configurable positive integer within [assignment: <i>range of acceptable values</i> ] unsuccessful authentication attempts occur related to [assignment: <i>list of authentication events</i> ].	
[assignment: <i>list of authentication events</i> ] : <b>Authentication by HDD Lock function at the time of accessing HDD</b>	
[selection: <i>assignment: positive integer number</i> ], an administrator configurable positive integer within [assignment: <i>range of acceptable values</i> ] <b>[assignment: <i>positive integer number</i>] : 5</b>	
FIA_AFL.1.2[E]	
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: <i>list of actions</i> ].	
[assignment: <i>list of actions</i> ] : < <b>Action when it is detected</b> > <b>Deny the reading and writing of data to HDD.</b> < <b>Operation for recovering the normal condition</b> > <b>Turn off electricity to HDD ( Power OFF )</b>	
Hierarchical to	: No other components
Dependencies	: FIA_UAU.1 ( FIA_UAU.2[E] )

<b>FIA_UAU.2[E]</b>	<b>User authentication before any action</b>
FIA_UAU.2.1[E]	
The <b>TSF (HDD)</b> shall require each <b>user ( The main body of MFP where HDD installed )</b> to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that <b>user ( The main body of MFP where HDD installed )</b> .	
Hierarchical to	: FIA_UAU.1
Dependencies	: FIA_UID.1 ( N/A )

<b>FIA_UAU.7[E]</b>	<b>Protected authentication feedback</b>
FIA_UAU.7.1[E]	
The <b>TSF (PC application)</b> shall provide only [assignment: <i>list of feedback</i> ] to the user while the authentication is in progress.	
[assignment: <i>list of feedback</i> ] : <b>display "*" in every character data input</b>	
Hierarchical to	: No other components
Dependencies	: FIA_UAU.1 ( FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.2[5] )

## 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
User Password	More than 8-digits	92 characters in total can be selected ASCII code ( 0x21 - 0x7E, except 0x22 and 0x2B ) • Number : 0 - 9
CE Password	8-digits	• 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
Secure Print Password		• Alphabets : Capital letter and small letter • Symbols : !, #, \$, %, &, ', (, ), *, , , - , . , / , : , ; , < , = , > , ? , @ , [ , ¥ , ] , ^ , _ , ` , { ,   , } , ~ , <i>SPACE</i>
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
Encryption passphrase		• Alphabets : Capital letter and small letter • Symbols : !, #, \$, %, &, ', (, ), *, , , - , . , / , : , ; , < , = , > , ? , @ , [ , ¥ , ] , ^ , _ , ` , { ,   , } , ~
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 : !, #, \$, %, &, ', (, ), *, , , - , . , / , : , ; , < , = , > , ? , @ , [ , ¥ , ] , ^ , _ , ` , { ,   , } , ~ , " , + , <i>SPACE</i>

#### 6.1.1.2. Auto logoff function of administrator mode

While accessing an administrator mode from a panel, if not accepting any operation during the panel automatic logoff time, it logs off the administrator mode automatically.

#### 6.1.1.3. 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.

### Change of Administrator password

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

- Offers the administrator 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.

### User Settings

#### ➤ User Registration

User is registered by setting the user ID and registering the user password. It verifies whether the user 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.

While the external server authentication is effective, the user password cannot be registered.

#### ➤ Change of user ID and user password

User ID and user password is changed. It verifies whether the user 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.

While the external server authentication is effective, the user ID and the user password cannot be changed, same as the user registration.

#### ➤ User deletion

User ID and user password is deleted.

- When a personal user box that a concerned user owns exists, that personal user box is automatically set to the public user box of "user attributes: public."

### User Box Settings

#### ➤ User Box Registration

The public user box of "user attributes: public" is registered for the selected unregistered user box ID.

- 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.
- Change of user attribute of user box
  - If the registered user is specified in the user attribute of a personal user box, the user box becomes a personal user box which the registered user manages. (personal another personal)
  - If the user attribute of a personal user box is specified as public, it becomes a public user box. (personal public)
    - ◇ The registration of a user box password is necessary at the same time, and then the processing which is similar to a change of the above-mentioned user box password should be done.

#### Release of Lock

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

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

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

- 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.

#### Setting of user authentication function

An authentication method in a user authentication function is set to the "machine authentication" which utilizes a user password managed in the main body of MFP side or to the "external server authentication" which utilizes a user password managed with a user information management server connected through a network. (When the external server authentication is used, the external server authentication setting data (domain name to which an external server belongs etc.) needs to be set.)

#### Setting of unauthorized access detection threshold

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

#### Setting and execution of all area overwrite deletion function

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

Table 7 HDD data deletion method of overwriting deletion at the all area of HDD

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							

#### Setting of auto logoff function

The panel auto logoff time which is the setting data of the auto logoff function should be set within the following time range.

- panel auto logoff time : 1 - 9 minutes

#### Network Settings

A setup operation of the following setting data is performed.

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

#### Execution of back-up and restoration function

All the setting data stored in NVRAM and 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 >

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

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

- A series of data that relates to SMTP server setting
- A series of data that relates to DNS server setting
- A series of data that relates to MFP address setting
- Setting data of Enhanced Security function
- Setting data of operation method of user authentication function
- Authentication failure frequency threshold of authentication operation prohibition function
- Panel auto logoff time

- User ID
- User attribute of user box

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

- Secure print file
- User box file

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.
  - It shall not be matched with the current value.

Operation setting of encryption function

When an optional encryption board is installed to MFP, 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.

- It shall not be matched with the current value.

#### 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 .)

- 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

#### 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.

#### 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 Table 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.

##### Network Settings

Setting operation of the following setting data is performed.

- Setting data that relates to SMTP server ( IP address, port number, etc. )
- Setting data that relates to DNS server ( IP address, port number, etc. )
- A series of setting data that relates to MFP address( IP address, NetBIOS name, AppleTalk printer name, etc. )

##### 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.

##### 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.

#### 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.

#### 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.

#### 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.
- Initialization function (setting of network)  
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.

Function that sets the actions of maintenance function (through LAN)

The function that sets the actions of maintenance function by the access through LAN. (It is possible to change the operation from hold state to active state.)

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 (setting of network)  
Function to reset various setting values written in NVRAM to the factory default. The SNMP password are set to an initial value of the factory shipment by executing this initialization function.
- 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.USER ( User Function )

F.USER identifies and authenticates the user for the use of MFP various function. To the identified and authenticated user, it offers the management function of the user password that is managed in the MFP at the time of machine authentication, besides the permission of the use of functions such as F.BOX and F.PRINT.

##### 6.1.4.1. User Identification and Authentication Function

< User identification and authentication >

When the access request for the user box and the request for the registration of the secure print file, it is identified and authenticated to be a user. The use of F.BOX and F.PRINT is permitted to the user who is identified and authenticated.

- Offers the user authentication mechanism that authenticates the user that consists of the characters shown in Table 6.
  - After the user is authenticated to the access from the network, the user authentication mechanism using session information besides the user password is offered.
  - According to the protocol, it uses the session information more than 10<sup>10</sup> or it generates

and uses the session information more than 10<sup>10</sup>.

- Return "\*" for each character as feedback for the entered user password.
- Resets the number of authentication failure when succeeding in the authentication.
- Not accept the access from the panel for five seconds when the authentication failed.
- When the authentication failure that becomes 1-3 times at total for the concerned user is detected, it locks all the authentication functions to the user.
  - The administrator specifies the failure frequency threshold by the unauthorized access detection threshold setting function.
- To release the lock of the authentication function is to perform the lock release function to the user authentication of F.ADMIN or to operate the F.RESET function.

< The user's automatic registration >

In the case of the "External server authentication" has been selected as the user authentic method, when the user who is identified and authenticated with the above-mentioned function is not registered in the MFP<sup>10</sup>, this user ID is registered.

#### 6.1.4.2. Auto logoff function in user identification and authentication domain

While the user who is identified and authenticated is accessing from a panel, if it does not accept any operations for more than the "panel automatic logoff time", it logs off from a user identification and authentication domain automatically.

#### 6.1.4.3. Modification function of user password

When the identification and authentication are succeeded, and the access to the user identification and authentication domain is permitted, the user is permitted to change its own password. When the external server authentication is effective, this function cannot be applied.

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

- 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.

#### 6.1.5. F.BOX ( User Box Function )

F.BOX is a series of security function related to the user box to the user who is identified and authenticated that you are the registered user, such as the permission of the operation and management of the personal user box of the user, the authentication to the user who is permitted the utilization of the user box in the access to the public box, and the access control function to permit various operations of the concerned user box and the user box file after the authentication.

< Registration of user box by user operation >

To register a personal user box or a public user box by selecting the user attribute to the non-registration user box ID selected. When it's registered, it is possible to select "User ID" in the user attribute of the user box which have been specified "Public" as a default value.

---

<sup>10</sup> Registration in the main body of MFP doesn't become a problem because it is a registered user in the trusted user information management server.

- In the case of the personal user box, the arbitrary user ID registered is specified.
- In the case of the public user box, 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.

< Automatic registration of user box >

- In the user box operation to store of the copy job and the print job, when the specified user box is unregistered, the personal user box which is set the user ID of the user who operates the job concerned is automatically registered.

#### 6.1.5.1. Personal User Box Function

Access control function to personal user box

The task to act for the identified and authenticated user has "User ID" of the user who is identified and authenticated for the user attribute. This task is permitted the display of the list of the personal user box which has a corresponding user attribute with this user attribute.

Access control function to a user box file in a personal user box

When the user box to operate is selected, "User Box ID" of the user box is related to the task as a user box attribute in addition to the user attribute. This task is permitted, to the user box file with the user attribute and the user box attribute corresponding to the user attribute and the user box attribute of itself, the printing, the E-mail transmission, the FTP transmission, the FAX transmission, the SMB transmission, download, the removing to other user boxes, and the copy operations to other user boxes.

User attribute change of a personal user box

The user attributes can be changed.

- If another registered user is specified, it becomes a personal user box that another user manages.
- If public is specified, it becomes a public user box. It is necessary to register the user box password. In this case, it is verified that the user box password meets 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.

#### 6.1.5.2. Public User Box Function

When the user is identified and authenticated as a registered user, the task to act for the user who is identified and authenticated has "User ID" of the identified and authenticated user as the user attribute. This task is permitted the display of the list of the public user box which is set the public as the user attribute. The operation specification of each public user box is as follows.

- Authentication function in access to a public user box  
For the access request for each public user box, after the above-mentioned verification function is operated, 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 public user box concerned, the authentication function to the public 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 public user box of F.ADMIN executed or by the operation of the F.RESET function.

The following is a function that the user who is permitted the use of the public user box is offered in the user box identification and authentication domain of the user box.

- Access control to a user box file in a public user box

The task to act for the user is related the "User Box ID" of the user box as a user box attribute in addition to the user attribute. This task is permitted the user box file, which have been set the public to the user attribute and have a corresponding user box attribute to the user box attribute of the subject attribute, to do the printing, the E-mail transmission, the FTP transmission, the fax transmission, the SMB transmission, download, the movement to other user boxes, and the copy operations to other user boxes.

- User attribute change of a public user box

The user attribute of the user box can be changed.

- Specify the registered user. And change to a personal user box for the registered user.

- Change of a public user box password

Change the user box password of the public 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.

### 6.1.6. 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 and displaying the list of 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 to the identified and authenticated user as a registered user.

#### 6.1.6.1. Authentication function by the secure print password

When the user is identified and authenticated as the registered user, 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 password 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.

#### 6.1.6.2. Access control function to a secure print file

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

- The task to act for the user who is identified and authenticated has the 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.

#### 6.1.6.3. Registration function of a secure print file

When it is authenticated as a registered user in the registration request of the secure print file, the user is permitted to register the secure print password with the concerned secure print file.

##### 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.

##### 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.

#### 6.1.7. 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
- Transmission address data file
- User ID
- User password
- 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.)

#### 6.1.8. 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 KonicaMinolta encryption specification standard. KonicaMinolta 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.

#### 6.1.9. 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.

#### 6.1.10. 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
- The number of failure to authentication of each public 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.

Administrator authentication mechanism, HDD lock password verification mechanism, and encryption passphrase verification mechanism which F.ADMIN offers  
CE authentication mechanism which F.SERVICE offers  
Secure print authentication mechanism which F.PRINT offers  
User box authentication mechanism which F.BOX offers  
SNMP authentication mechanism which F.ADMIN-SNMP offers  
User authentication mechanism which F.USER 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	<ul style="list-style-type: none"> <li>• Configuration management plan</li> <li>• Configuration List</li> <li>• CM record</li> </ul>
	CM scope	ACM_SCP.1	
Class ADO: Delivery and Operation	Delivery	ADO_DEL.1	Delivery/Operation instructions
	Installation, generation and start-up	ADO_IGS.1	<ul style="list-style-type: none"> <li>• Service Manual bizhub 500 / 420 Service Manual [Security Function] (Japanese), bizhub 500 / 420 ineo 500 / 420 Service Manual [Security Function] (English)</li> <li>• Users Guide bizhub 500 Users Guide [Security Operations] (Japanese), bizhub 420 Users Guide [Security Operations] (Japanese), bizhub 500 User's Guide [Security Operations] (English), bizhub 420 User's Guide [Security Operations] (English), ineo 500 / 420 User's Guide [Security Operations] (English)</li> </ul>
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	<ul style="list-style-type: none"> <li>• Service Manual bizhub 500 / 420 Service Manual [Security Function] (Japanese), bizhub 500 / 420 ineo 500 / 420 Service Manual [Security Function] (English)</li> <li>• Users Guide bizhub 500 Users Guide [Security Operations] (Japanese), bizhub 420 Users Guide [Security Operations] (Japanese), bizhub 500 User's Guide [Security Operations] (English), bizhub 420 User's Guide [Security Operations] (English), ineo 500 / 420 User's Guide [Security Operations] (English)</li> </ul>
	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 (including results report)
	Independent testing	ATE_IND.2	MFP 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	A.ADMIN	A.SERVICE	A.NETWORK	A.SECRET	A.SETTING	A.SERVER	T.DISCARD-MFP	T.BRING-OUT-STORAGE	T.ACCESS-PRIVATE-BOX	T.ACCESS-PUBLIC-BOX	T.ACCESS-SECURE-PRINT	T.ACCESS-NET-SETTING	T.ACCESS-SETTING	T.BACKUP-RESTORE
Security objectives														
O.REGISTERED-USER														
O.PRIVATE-BOX														
O.PUBLIC-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.SERVER														
OE-N.SESSON														
OE-N.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 MFP assigns personnel who are reliable in the organization that uses the MFP, so the reliability of the administrator is realized.

- **A.SERVICE ( Personnel Conditions to be a Service Engineer )**

This condition assumes the service engineer are not malicious.

With OE-N.SERVICE, the organization that manages the maintenance of the MFP educates the service engineer. Also the administrator needs to observe the maintenance of the MFP, so that the reliability of service engineers is assured.

- **A.NETWORK ( Network Connection Conditions for the MFP )**

This condition assumes that there are no wiretapping activities for the intra-office LAN and no access by an unspecified person from an external network.

OE-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 MFP from the external networks, so that this condition is realized.

- **A.SECRET ( Operating condition concerning confidential information )**

This condition assumes each password and encryption 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, the user box password and user 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 ( MFP Operational Settings Condition for Enhanced Security Function etc. )**

This condition assumes the enhanced security function operational settings condition and prohibition setting of maintenance function(through LAN) are satisfied.

OE-N.SETTING-SECURITY regulates that this is used after the administrator activates the enhanced security function and prohibits the maintenance function(through LAN), so that this condition is realized.

- **A.SERVER ( Management condition of user information management server connected with the intra-official LAN )**

This condition assumes that the requiring user information management server is managed securely when "external server authentication" is used as the method of the user authentication.

OE-N.SERVER regulates that the person in charge of the organization executes the server management which is necessary to maintain security such as the patch application, the account management, and the access control for the user information management serve, so that this condition is realized.

### 8.1.3. Sufficiency of Threats

The security objectives against threats are described as follows.

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

This threat assumes the possibility of leaking information from HDD inside MFP 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 MFP 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 MFP 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.

O.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.

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

In the above-mentioned, when only is selected, danger of leaking exists by taking out the another HDD without the function of 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-PRIVATE-BOX ( Unauthorized access to personal user box using user function )**

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

O.REGISTERED-USER is assumed that only the user to whom TOE was registered is permitted to use MFP installed TOE, furthermore, the operation of a personal user box and the user box file in a personal user box is restricted only to the user who is the owner by O.PRIVATE-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's authentication, and OE-N.SESSIOIN also requires the log-off operation after the operation ends, so that O.REGISTERED-USER and O.PRIVATE-BOX are supported sufficiently.

Accordingly, this threat is countered sufficiently.

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

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

O.REGISTERED-USER assumes that only the user to whom TOE was registered is permitted to use MFP installing TOE, furthermore, the operation of the public user box and the user box file in the public user box is restricted only to the user who is permitted by O.PUBLIC-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's authentication and user box's authentication, and OE-N.SESSION requires the log-off operation after the operation ends, so that O.REGISTERED-USER and O.PUBLIC-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.

O.REGISTERED-USER assumes that only the user to whom TOE was registered is permitted to use MFP installing TOE, furthermore, 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 user's authentication and access authentication to the secure print, and OE-N.SESSION requires the log-off operation after the operation ends, so that O.REGISTERED-USER and 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 of sending the user box file to the address that isn't intended, when the network setting that relates to the transmission is illegally changed. This is concerned about a possibility that the user box file is transmitted to the specified server illegally without the change of the network environment constitution by the malicious person by, for instance, illegally being changed the address of the SMTP server that relays E-mail for the E-mail, or illegally being changed the address of the DNS server where the domain name is inquired when the address of the SMTP server is used for a search of the domain name. For FTP transmission, by being likely to use the mechanism of the search of the domain name is concerned about the similar possibility of the incident might be occurred by E-mailing.

Furthermore, when the network setting which is related to the address of MFP is modified illegally, it assumes the possibility to use the print function to the unauthorized entity from PC by the user who believes as TOE. Especially, it becomes a problem if a secure print file which is required to be concealed from other users in the office is transmitted to the unauthorized entity.

On the other hand, O.CONFIG regulates that the role to operate the network setting relating to the transmission of TOE is limited to the administrator, and so the possibility of this threat is removed.

OE.FEED-BACK regulates that the 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.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-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
<b>set.admin</b>													
<b>set.service</b>													
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_AFL.1[7]													
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.1[6]													
FIA_SOS.2													
FIA_UAU.2[1]													
FIA_UAU.2[2]													
FIA_UAU.2[3]													
FIA_UAU.2[4]													
FIA_UAU.2[5]													
FIA_UAU.6													
FIA_UAU.7													
FIA_UID.2[1]													
FIA_UID.2[2]													
FIA_UID.2[3]													
FIA_UID.2[4]													
FIA_UID.2[5]													
FIA_UID.2[6]													
FIA_USB.1													
FMT_MOF.1[1]													
FMT_MOF.1[2]													
FMT_MOF.1[3]													
FMT_MSA.1[1]													
FMT_MSA.1[2]													
FMT_MSA.3[1]													
FMT_MSA.3[2]													

Security Objective / Security Functional Requirements	O.REGISTERED-USER	O.PRIVATE-BOX	O.PUBLIC-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[1]													
FMT_MTD.1[2]													
FMT_MTD.1[3]													
FMT_MTD.1[4]													
FMT_MTD.1[5]													
FMT_MTD.1[6]													
FMT_MTD.1[7]													
FMT_MTD.1[8]													
FMT_MTD.1[9]													
FMT_MTD.1[10]													
FMT_MTD.1[11]													
FMT_MTD.1[12]													
FMT_SMF.1													
FMT_SMR.1[1]													
FMT_SMR.1[2]													
FMT_SMR.1[3]													
FMT_SMR.1[4]													
FMT_SMR.1[5]													
FPT_RVM.1													
FPT_SEP.1													
FTA_SSL.3													
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.REGISTERED-USER ( Usage of a registered user )**

This security objective limits the utilization of MFP installing TOE to only the registered user, and needs various requirements that related to the user identification and authentication.

< Necessary requirement for identification and authentication of the user >

It identifies and authenticates that the user who accesses is a registered user by

FIA\_UID.2[3] and FIA\_UAU.2[3].

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 [7] 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] 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\_MOF.1[2] permits only the administrator the selection of the user authentication methods which are "Machine authentication" and "External server authentication". FMT\_MTD.1[3] permits only the administrator the setting of the threshold of the unauthorized access detection value which is the trial frequency of the failure authentication in the user authentication (modification).

< Necessary requirements for managing session of user who is identified and authenticated >

The duration of session of the user who is identified and authenticated contributes to reduce the chance of attacking associated with unnecessary session connection, by ending the session after the panel automatic logoff time elapses with FTA\_SSL.3. when it logs in from the panel. The change in the panel auto logoff time is limited to the administrator by FMT\_MTD.1[3].

< Necessary requirement for managing the identification and authentication information of the user >

When "the machine authentication" is chosen in a method of the user authentication by FMT\_MTD.1[1], the initial registration of a user password in the user's registration is permitted only by the administrator.

When "the machine authentication" has been selected in the method of the user authentication, the registration of the user ID in the user registration is permitted to the administrator by FMT\_MTD.1[10]. When the "external server authentication" (has been selected in the user authentication method, the user who is authenticated the identification is permitted from an external server and registered automatically by this requirement. ( This corresponds to the user ID registration of the "external server". ) At this registration, the external server accessing TOE is identified the external server registered by FIA\_UID.2[6]. This management behavior is maintained as the role of the external server by FMT\_SMR.1 [5]. In addition, the registration function of user ID is specified for the administration function by FMT\_SMF.1.

The setting change operation of an external server is limited to only the administrator by FMT\_MTD.1[3].

The quality of the user password is verified by FIA\_SOS.1[3]. In addition, the quality of session information used in the user authentication via the network by FIA\_SOS.1[6] is verified, and the quality of session information that is generated with FIA\_SOS.2 is secured. When "machine authentication" is selected in the method of the user authentication, a change of the user password is limited to the user itself and the administrator by FMT\_MTD.1[2]. The change of the user ID is limited only to the administrator by FMT\_MTD.1[3].

< 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 management function for each management >

The role to do these managements is maintained as an administrator by FMT\_SMR.1[2] and a user by FMT\_SMR.1[3]. Moreover, these management functions are specified by FMT\_SMF.1.

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

● **O.PRIVATE-BOX ( personal user box access control )**

This security objective limits access to the personal user box and the user box file in the personal 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 personal user box) >

By FDP\_ACC.1[1] and FDP\_ACF.1[1], the task of acting the user has a user ID, and is permitted to display the list of the user box with a corresponding user attribute. In addition, after the user box has been selected, when the user box ID is related to the task of acting a use by FIA\_ATD.1 and FIA\_USB.1, the operation such as a print, a download, transmissions, a movement, and a copy is permitted to the user box file that has a corresponding object attribute to user ID and user box ID of the subject attribute.

< Management of a personal user box >

FMT\_MSA.1[1] permits to the user and the administrator the change operation of the user attribute of the user box where the user ID is set.

As for the registration of the user box, public is appointed to the user attribute of the user box by FMT\_MSA.3[1], and it is permitted only to the user being able to give the initial value to change. In addition, when the job to store the non-registered user box into the user box appointed is executed due to the same requirement, a user ID of the user who executes a job concerned is appointed automatically.

< 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.PUBLIC-BOX ( a public user box access control )**

This security objective permits the inspection of the public user box to all users, and limits the setting of the public user box and the operation of the user box file in the public user box only to the user who permitted the utilization of that public user box. And it needs the various requirements that related to the access control.

< User box access control (a public user box) >

FDP\_ACC.1[1] and FDP\_ACF.1[1] permits the list display operation to the user box where public is set to the user attribute to the task of acting the user who has user ID.

It is required to be a user who is permitted the use of the user box to operate the user box file in the public user box. FIA\_UID.2[5] and FIA\_UAU.2[5] 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 [7] refuses all input acceptances from the panel for 5 seconds in every failure. When the authentication failure reaches 1-3 times, FIA\_AFL.1 [6] 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[3] 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 and is set public to the user attribute of user box, the operation such as a print, a download, transmissions, a movement, and a copy.

< Management of a public user box >

FMT\_MSA.1[2] permits the user who is permitted the use of the user box to operate the change of the user attribute of use box which "Public" is set. FMT\_MTD.1[4] 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[5] verifies the quality of the user box password. Moreover, FIA\_SOS.1[6] 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.

As for the user box registration, FMT\_MSA.3 specifies the public to the user attribute of the user box, and permits only the user to be given the initial value to change it. Moreover, when the job that stores an unregistered user box in the box where is specified by this requirement is executed, the user ID of the user who executed a job concerned is automatically specified. FMT\_MTD.1[5] permits the registration of the user box password only to the user or 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[2] maintains an administrator and FMT\_SMR.1[4] 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 >

FDP\_ACC.1[2] and FDP\_ACF.1[2] permits the list display operation of every secure print user box to the task of acting the user who has user ID.

As it must be a user who is permitted the use of the secure print file to print it, FIA\_UID.2[4] and FIA\_UAU.2[4] 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 [7] refuses all input acceptances from the panel for 5 seconds in every failure. When the authentication failure reaches 3 times, FIA\_AFL.1 [5] 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[3] 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[2] gives the value uniquely identified when the secure print file is registered.

< Secure print password >

FMT\_MTD.1[8] permits only to the user the registration of the secure print password used for the authentication. FIA\_SOS.1[5] 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 and FMT\_SMR.1[3] maintains a user. 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 SMTP server, the setting related to the DNS server, the setting related to the Enhanced Security function, the backup function, the restorations function to the administrator and the setting of the Enhanced Security function to the administrator and the service engineer, 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 SMTP server group object, the DNS server group object and the settings for the MFP 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 by FDP\_ACC.1[3] and FDP\_ACF.1[3].

In addition, the restoration operation is permitted for

- the encryption passphrase object, the SMTP server group object, the DNS server group object, and the MFP 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 user attribute of the user box by FMT\_MSA.1[1] and FMT\_MSA.1[2].
- the user password by FMT\_MTD.1[2].
- the user ID, the SNMP password, the panel auto logoff time, the authentication failure frequency, the secure print password by FMT\_MTD.1[3].
- the user box password by FMT\_MTD.1[4].

FMT\_MTD.1[7] permits only to the administrator the backup operation (inquiry operation) of the SNMP password, the user 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 activate the maintenance function(through LAN).

< 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[4] 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 object. 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 to the task of acting the user.

< Necessary requirement for accessing MIB object >

The SMTP server group object, the DNS server group object and the MFP 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] identifies and authenticates 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[3] 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[3] restricts the change in the SNMP password to the administrator. FIA\_SOS.1[2] verifies the quality of the SNMP password.

FMT\_MTD.1[11] 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 KonicaMinolta HDD encryption key generation mechanism (SHA-1) according to KonicaMinolta encryption specification standard, FCS\_CKM.1 generates the 128bit encryption key. KonicaMinolta 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 MFP 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 right MFP where TOE is installed.

By FIA\_UAU.2[E], HDD authenticates that the entity accessing to HDD is MFP, 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 MFP) that is the entity of a necessary IT environment for the TOE security maintenance offers the appropriate protected feedback for the entered use password, 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 the set of necessary requirement to keep administrator secure (set.admin), the set of necessary requirement to keep service engineer secure (set.service).

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

< Identification and Authentication of an administrator >

FIA\_UID.2[2] and FIA\_UAU.2[2] identifies and authenticates that the accessing user is an administrator.

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

FIA\_AFL.1[7] 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] logoffs if it's under authentication, and 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[3] 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 session of identified and authenticated administrator >

The duration of session of the administrator who is identified and authenticated contributes to reduce the chance of attacking associated with unnecessary session connection by ending the session after the panel automatic logoff time elapses by FTA\_SSL.3. if it logs in from the panel. The change in the panel auto logoff time is limited to the administrator by FMT\_MTD.1[3].

< Management of administrator's authentication information >

FIA\_SOS.1[1] verifies the quality of the administrator password. Moreover, FIA\_SOS.[6] 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[6] 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] logoffs it if it's under authentication, and logoffs and releases

the authentication status of the administrator from then on. And afterthat 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[12] restricts the initialization of the administrator password to the administrator.

< 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[7] 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] logoffs it if it's under authentication, 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.

FMT\_MTD.1[3] 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[9] 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] logoffs 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 immediately 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 approval 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 apply FCS_CKM.4, FMT_MSA.2 > 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. 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], FMT_MSA.3[1]
FDP_ACF.1[2]	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1[2], FMT_MSA.3[2]
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[5]
FIA_AFL.1[7]	FIA_UAU.1	FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.2[4], FIA_UAU.2[5]
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.1[6]	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]
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3]
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[4]
FIA_UAU.2[5]	FIA_UID.1	FIA_UID.2[5]
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_UAU.2[5]
FIA_UID.2[1]	None	N/A

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FIA_UID.2[2]	None	N/A
FIA_UID.2[3]	None	N/A
FIA_UID.2[4]	None	N/A
FIA_UID.2[5]	None	N/A
FIA_UID.2[6]	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.1[1]	FDP_ACC.1 or FDP_IFC.1, FMT_SMF.1, FMT_SMR.1	FDP_ACC.1[1], FMT_SMF.1, FMT_SMR.1[2], FMT_SMR.1[3]
FMT_MSA.1[2]	FDP_ACC.1 or FDP_IFC.1, FMT_SMF.1, FMT_SMR.1	FDP_ACC.1[1], FMT_SMF.1, FMT_SMR.1[2], FMT_SMR.1[4]
FMT_MSA.3[1]	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_MTD.1[7]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MTD.1[8]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[3]
FMT_MTD.1[9]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]
FMT_MTD.1[10]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2], FMT_SMR.1[5]
FMT_MTD.1[11]	FMT_SMF.1	FMT_SMF.1

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
	FMT_SMR.1	FMT_SMR.1[1] FMT_SMR.1[2]
FMT_MTD.1[12]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.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[3]
FMT_SMR.1[4]	FIA_UID.1	FIA_UID.2[5]
FMT_SMR.1[5]	FIA_UID.1	FIA_UID.2[6]
FPT_RVM.1	None	N/A
FPT_SEP.1	None	N/A
FTA_SSL.3	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 apply FCS_CKM.4, FMT_MSA.2 > 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. 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 MFP. 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[3], FIA_UAU.2[5]

### 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			
	Bypass Prevention	Interference/ Destruction Prevention	Deactivation Prevention	Disabling Detection
FCS_CKM.1	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FDP_ACC.1[1]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FDP_ACC.1[2]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FDP_ACC.1[3]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FDP_ACF.1[1]	FIA_UAU.2[2] FIA_UAU.2[3] FIA_UAU.2[5]	FMT_MSA.1[1] FMT_MSA.1[2] FPT_SEP.1	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FDP_ACF.1[2]	FIA_UAU.2[2] FIA_UAU.2[3] FIA_UAU.2[4]	FPT_SEP.1	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FDP_ACF.1[3]	FIA_UAU.2[1] FIA_UAU.2[2]	FPT_SEP.1	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_AFL.1[1]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_AFL.1[2]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_AFL.1[3]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_AFL.1[4]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_AFL.1[5]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_AFL.1[6]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_AFL.1[7]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_ATD.1	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_SOS.1[1]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_SOS.1[2]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_SOS.1[3]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_SOS.1[4]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_SOS.1[5]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_SOS.1[6]	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[9]	FMT_MOF.1[1]	N/A

IT Security Functional Requirement	Functional requirement component that operates other security functional requirements validly			
	Bypass Prevention	Interference/ Destruction Prevention	Deactivation Prevention	Disabling Detection
			FMT_MOF.1[3]	
FIA_UAU.2[2]	FPT_RVM.1	FMT_MTD.1[3] FMT_MTD.1[6] FMT_MTD.1[7] FMT_MTD.1[11] FMT_MTD.1[12]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UAU.2[3]	FPT_RVM.1	FMT_MTD.1[1] FMT_MTD.1[2] FMT_MTD.1[7]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UAU.2[4]	FPT_RVM.1	FMT_MTD.1[3] FMT_MTD.1[7] FMT_MTD.1[8]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UAU.2[5]	FPT_RVM.1	FMT_MTD.1[4] FMT_MTD.1[5] FMT_MTD.1[7]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UAU.6	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UAU.7	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UID.2[1]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UID.2[2]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UID.2[3]	N/A	FMT_MTD.1[3] FMT_MTD.1[10]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UID.2[4]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UID.2[5]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UID.2[6]	N/A	FMT_MTD.1[3]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_USB.1	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	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] FMT_MOF.1[3]	N/A
FMT_MOF.1[3]	N/A	N/A	N/A	N/A
FMT_MSA.1[1]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MSA.1[2]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MSA.3[1]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MSA.3[2]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MTD.1[1]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MTD.1[2]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MTD.1[3]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MTD.1[4]	N/A	N/A	FMT_MOF.1[1]	N/A

IT Security Functional Requirement	Functional requirement component that operates other security functional requirements validly			
	Bypass Prevention	Interference/ Destruction Prevention	Deactivation Prevention	Disabling Detection
			FMT_MOF.1[3]	
FMT_MTD.1[5]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MTD.1[6]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MTD.1[7]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MTD.1[8]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MTD.1[9]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MTD.1[10]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MTD.1[11]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_MTD.1[12]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_SMF.1	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_SMR.1[1]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_SMR.1[2]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_SMR.1[3]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_SMR.1[4]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FMT_SMR.1[5]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FPT_RVM.1	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FPT_SEP.1	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FTA_SSL.3	N/A	FMT_MTD.1[3]	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_NEW.1	FPT_RVM.1	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FNEW_RIP.1	N/A	N/A	N/A	N/A
FCS_COP.1[E]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_AFL.1[E]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UAU.2[E]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A
FIA_UAU.7[E]	N/A	N/A	FMT_MOF.1[1] FMT_MOF.1[3]	N/A

## Bypass Prevention

< 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 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 setting management access control, the by-pass prevention is supported by FIA\_UAU.2[2] that regulates the administrator's identification and authentication.

In addition, 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 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[3] that regulates the authentication of the user. FIA\_UAU.2[5] also contributes to the by-pass prevention of FDP\_ACF.1[1] for the access to the public user box.

In addition, because FIA\_UAU.2[3] that regulates the authentication of the user and FIA\_UAU.2[5] that regulates the authentication of the user who is permitted the use of the public 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 regulates the authentication of the user and FIA\_UAU.2[4] that authenticates the authorized user to use the secure print file.

In addition, because FIA\_UAU.2[3] that regulates the authentication of the user and FIA\_UAU.2[4] 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.

## Interference and Destruction Prevention

< Maintenance of user box access control >

The user attribute that is the security attribute of the user box, when "Public" is set, permits the modification only to the user who is allowed to use the user box or the administrator by FMT\_MSA.1[2]. When "User ID" is set, FMT\_MSA.1[1] permits the modification only to the user and the administrator. Moreover, by FPT\_SEP.1, only the subject of three types such as the authenticated user who is assumed by the user box access control, the authenticated administrator, and the user who is permitted the use of the authenticated public user box, can operate the user box and the user box file.

With three 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 three types of subject which are the authenticated user who is assumed by the secure print file access control, the authenticated administrator, and the authenticated user who is permitted the use of 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[9]. 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[6]. The initialization of the administrator password is permitted only to the administrator by FMT\_MTD.1[11]. 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[3]. The inquiry operation is permitted to the administrator by FMT\_MTD.1[7], and the initialization operation is permitted only to the administrator and the service engineer by FMT\_MTD.1[11]. This supports the prevention of unauthorized interference and destruction of FIA\_UAU.2[2].

< Management of user password >

The registration of the user password is permitted to the administrator by FMT\_MTD.1[1]. The modification operation is permitted to the administrator and the user by FMT\_MTD.1[2], and the inquiry operation is permitted only to the administrator by FMT\_MTD.1[7]. This supports the prevention of unauthorized interference and destruction of FIA\_UAU.2[3].

< Management of secure print password >

The registration of the secure print password is permitted only to the user by FMT\_MTD.1[8], and the inquiry operation is permitted only to the administrator by FMT\_MTD.1[7]. The modification is permitted only to the administrator by FMT\_MTD.1[3]. This supports the prevention of unauthorized interference and destruction of FIA\_UAU.2[4].

< Management of user box password >

The registration of the user box password is permitted to the administrator and the user by

FMT\_MTD.1[5], and the modification operation is permitted to the administrator and the user who is permitted the use of the public user box by FMT\_MTD.1[4]. The inquiry operation is permitted only to the administrator by FMT\_MTD.1[7]. This supports the prevention of unauthorized interference and destruction of FIA\_UAU.2[5].

< Management of user ID >

The registration of user ID is limited only to the administrator by FMT\_MTD.1[10], and when the external server authentication is used, the user who is not registered in MFP is automatically registered with successful user authentication. Moreover, FMT\_MTD.1[3] permits the modification operation only to the administrator. This supports the prevention of unauthorized interference and destruction of FIA\_UID.2[3].

< Management of setting data for the external server authentication >

The setting of the external server authentication setting data used for the external server authentication is permitted only to the administrator by FMT\_MTD.1[10]. This supports the prevention of unauthorized interference and destruction of FIA\_UID.2[6].

< Management of auto logoff time >

FMT\_MTD.1[3] permits the modification operation of the panel auto logoff time only to the administrator. This supports the prevention of unauthorized interference and destruction of FTA\_SSL.3.

< 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 user authentication, the secure print authentication, the user authentication, and the MIB object access authentication is permitted only to the administrator by FMT\_MTD.1[3]. This supports the prevention of unauthorized interference and destruction of FIA\_AFL.1[1], FIA\_AFL.1[2], FIA\_AFL.1[3], FIA\_AFL.1[4], FIA\_AFL.1[5], FIA\_AFL.1[6].

## 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. FMT\_MOF.1[3] permits only to the service engineer the operation setting of the maintenance function(through LAN). The Enhanced Security function and the maintenance function(through LAN) influences all the security structures of TOE except the all area overwrite deletion function, the detection of the quality of session information and the detection of TOE falsification executed by the specified operation of the administrator, and This supports the deactivation prevention of all the security functions achieved by the security requirements of TOE except FNEW\_RIP.1, FIA\_SOS.1[6], FIS\_SOS.2, FMT\_MOF.1[1] and FMT\_MOF.1[3].

## Disabling Detection

The requirement that supports the disabling detection doesn't exist.<sup>11</sup>

<sup>11</sup> 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

### 8.2.2. Rational for Minimum Strength of Function

The MFP 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 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.

< IT security functional requirement >

- Though several access control policies are set up by repeating the access control requirement (FDP\_ACC.1 etc.), and it regulates the access control related to the followings, such as user box, secure print, MFP 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

---

security objective of this TOE. (This content is specified by the dependency analysis.)

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.USER	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]										
FIA_AFL.1[6]										
FIA_AFL.1[7]										
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.1[6]										
FIA_SOS.2										
FIA_UAU.2[1]										
FIA_UAU.2[2]										
FIA_UAU.2[3]										
FIA_UAU.2[4]										
FIA_UAU.2[5]										
FIA_UAU.6										
FIA_UAU.7										

TOE Security Function TOE Security Functional Requirement	F.ADMIN	F.ADMIN-SNMP	F.SERVICE	F.USER	F.BOX	F.PRINT	F.OVERWRITE-ALL	F.CRYPT	F.HDD	F.RESET
FIA_UID.2[1]										
FIA_UID.2[2]										
FIA_UID.2[3]										
FIA_UID.2[4]										
FIA_UID.2[5]										
FIA_UID.2[6]										
FIA_USB.1										
FMT_MOF.1[1]										
FMT_MOF.1[2]										
FMT_MOF.1[3]										
FMT_MSA.1[1]										
FMT_MSA.1[2]										
FMT_MSA.3[1]										
FMT_MSA.3[2]										
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_MTD.1[7]										
FMT_MTD.1[8]										
FMT_MTD.1[9]										
FMT_MTD.1[10]										
FMT_MTD.1[11]										
FMT_MTD.1[12]										
FMT_SMF.1										
FMT_SMR.1[1]										
FMT_SMR.1[2]										
FMT_SMR.1[3]										
FMT_SMR.1[4]										
FMT_SMR.1[5]										
FPT_RVM.1										
FPT_SEP.1										
FTA_SSL.3										
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 KonicaMinolta 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 display the list of user box and back-up the user box file.

F.BOX performs the user box access control for the task of acting for the user to display the list of the user box, print a user box file, transmit, download, move, and copy.

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 display and 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, SMTP server group object, DNS server group object and MFP 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 the HDD lock password object and encryption passphrase object. (The encryption passphrase object has also backup and restore operation.) In addition, it performs the setting management access control for the task of substituting the user to set and restore SMTP server group object, DNS server group object and MFP address group object.

F.ADMIN-SNMP performs the setting management access control for the task of substituting the user to set SMTP server group object, DNS server group object and MFP address group object.

F.SERVICE performs the setting management access control for the task of substituting the user to set HDD lock password 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 and 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 list display operation of the user box on the occasion of the user box setting.
- 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 list display of the user box (personal user box) that has a corresponding object attribute to user ID.
- It permits the user the operation of the user box file in the selected personal user box such as the print, the transmission, the download, the movement and the copy.
- It permits the user the list display operation of the user box (public user box) that sharing is set.
- It permits the user who is permitted the use of a user box the operation of user box file in the selected public user box such as the print, the transmission, the download, 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 user the list display operation of the secure print file.
- 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, the SMTP server group object, the DNS server group object and the MFP 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 encryption passphrase object.
- It permits the administrator the setting operation of the HDD lock password object.
- It permits the administrator the setting and the restoration operations of the SMTP server group object, the DNS server group object and the MFP 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 SMTP server group object, the DNS server group object and the MFP 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 (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 service code, 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 when it is under authentication status.

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 when it is under authentication status.

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 locks an authentication function for the access to the MIB object.

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[4]**

FIA\_AFL.1[4] regulates the action for the authentication failure to the authentication of the user. In the user authentication for accessing of user or changing the user password by user, when the authentication failure of failure frequency threshold (1-3 times) that the administrator sets is detected, F.USER logs off if it's under the authentication status and locks the authentication function of the concerned user from then on.

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 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[6]**

FIA\_AFL.1[6] regulates the action for the authentication failure to the authentication of the user permitted the use of the public user box. In the authentication for accessing the public user box and changing a public user box password, when the authentication failure of failure frequency threshold (1-3 times) that an administrator sets is detected, F.BOX 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[7]**

FIA\_AFL.1[7] 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 rejects 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.USER rejects all input receipts from a panel when the authentication failure is detected in the user authentication for the access of user from a panel.

F.BOX rejects all input receipts from a pane when the authentication failure is detected in the authentication for accessing to the public 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 user box ID to the task of substituting the user.

F.PRINT assigns the internal control ID of the secure print 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 user password.

F.ADMIN verifies that the quality of the user password is composed of ASCII code (0x21-0x7E, except 0x22 and 0x2B) in total of 92 characters by eight or more digits. Also it verifies that the first 8 characters are not composed of one kind of characters and it does not correspond to the value currently set.

F.USER verifies that the quality of the user password is composed of ASCII code (0x21-0x7E, except 0x22 and 0x2B) in total of 92 characters by eight or more digits. Also it verifies that the first 8 characters are not composed of one kind of characters and it does not correspond to the value currently set.

Accordingly, this functional requirement is satisfied.

- **FIA\_SOS.1[4]**

FIA\_SOS.1[4] 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, 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[5]**

FIA\_SOS.1[5] regulates the quality of the secure print password and the user box password.

F.ADMIN verifies that the quality of the secure print password and the user box password is composed of ASCII code (0x21-0x7E, 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 secure print password and the user box password is composed of ASCII code (0x21-0x7E, 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 and the user box password is composed of ASCII code (0x21-0x7E, 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[6]**

FIA\_SOS.1[6] 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.

F.USER 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.

F.USER generates the secrets that are the space quality of  $10^{10}$  or more to session information in the user 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 User.

F.USER authenticates that the user is the user who is registered by using the user password that is set to each user.

Accordingly, this functional requirement is satisfied.

- **FIA\_UAU.2[4]**

FIA\_UAU.2[4] 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 file.

Accordingly, this functional requirement is satisfied.

- **FIA\_UAU.2[5]**

FIA\_UAU.2[5] regulates the authentication of the authorized user to use the public user box.

F.BOX authenticates that the user is the authorized user to use the public 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.USER returns "\*" for each character for the entered user password from the panel in the authentication of the user, and prevents a direct display of the user 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 identification 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.

F.USER identifies the user who is registered by the user ID that is set to each user.  
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 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[5]**

FIA\_UID.2[5] regulates the identification of the user who is permitted the use of the public user box.

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

Accordingly, this functional requirement is satisfied.

- **FIA\_UID.2[6]**

FIA\_UID.2[6] regulates the identification of the external server.

F.USER identifies the external server which is accessed for the inquiry of user information when the external server authentication is selected for the user authentication method.

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 print internal control ID" to the task of substituting the user.

F.BOX associates the "User Box ID" to the task of substituting the user.

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 and initialization function(network setting) 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 user authentication and the SNMP password authentication.

F.ADMIN offers a setting function of the user authentication function in the administrator

mode, and permits the setting of the operational 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 maintenance function(through LAN).

F.SERVICE offers a activation and deactivation function of the maintenance function(through LAN) in the service more, and manages the operational mode of maintenance function(through LAN).

Accordingly, this functional requirement is satisfied.

- **FMT\_MSA.1[1]**

FMT\_MSA.1[1] regulates the management of the user attribute of user box (When user ID is set).

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

In addition, when a user concerned owns a personal user box by the deletion operation of registered user, the user box is changed to the public user box.

F.BOX permits the authenticated user the change of the user attribute of the user box where the user ID of the user concerned is set.

Accordingly, this functional requirement is satisfied.

- **FMT\_MSA.1[2]**

FMT\_MSA.1[2] regulates the management of the user attribute of user box (When public is set).

F.ADMIN permits the administrator the back-up and restoration operation, so that it is possible to change the back-up data which is acquired by the back-up operation and to change the user attribute of the user box as a result of restoration.

F.BOX permits the change of the user attribute of the user box where the public is set to the authenticated user who is permitted the use of the public user box.

Accordingly, this functional requirement is satisfied.

- **FMT\_MSA.3[1]**

FMT\_MSA.3[1] regulates the default value of the user attribute that is the security attribute given when the user box is generated.

F.ADMIN sets "public" to the user attribute of the user box as a default value in the user box registration operation that is executed in the administrator mode. (The administrator cannot change.)

F.BOX sets "public" to the user attribute of the user box as a default value in the user box registration operation that is executed by the authenticated user. User permits the change this to any value (user ID of the registered user).

In addition, when the job which is stored to the user box which specifies the unregistered user box is performed, the "User ID" of the user who executes the job concerned is set as a default

value and is stored to the unregistered user box. (The case of the specifying the unregistered user box cannot change the user attribute because there is no timing to set an initial value where the default value is changed.)

Accordingly, this functional requirement is satisfied.

**FMT\_MSA.3[2]**

FMT\_MSA.3[2] 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 the user password.

When "Machine authentication" is selected as the method of the user authentication, F.ADMIN offers the registration operation of the user password regarding the user registration in the administrator mode. In addition, F.ADMIN permits the administrator the back-up and restoration operation, so that it is possible to change the back-up data which is acquired by back-up operation and to register the user password as a result of performing the restoration operation.

Accordingly, this functional requirement is satisfied.

● **FMT\_MTD.1[2]**

FMT\_MTD.1[2] regulates the management of the user password.

When "Machine authentication" is selected as the method of the user authentication, F.ADMIN offers the change of the user password registered in the administrator mode. In addition, F.ADMIN permits the administrator back-up and restoration operation, so that it is possible to change the back-up data which is acquired by back-up operation and to change the user password as a result of performing the restoration operation.

When "Machine authentication" is selected as the method of the user authentication, F.USER permits the authenticated user the change of user's own password.

Accordingly, this functional requirement is satisfied.

● **FMT\_MTD.1[3]**

FMT\_MTD.1[3] regulates the management of a user ID, a SNMP password, the panel auto logoff time, the failure number of times threshold, and a secure print password.

F.ADMIN permits the operation to change the user ID, the SNMP password, the panel auto logoff time, the setting data of authentication failure frequency threshold and the setting data of the external server authentication 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 user ID, a SNMP password, the panel auto logoff time, the failure number of times threshold and a secure print password as a result of performing the restoration operation.

F.ADMIN-SNMP permits the change operation of the SNMP password to the administrator authenticated by the SNMP password.

Accordingly, this functional requirement is satisfied.

- **FMT\_MTD.1[4]**

FMT\_MTD.1[4] regulates the management of the user box password.

F.ADMIN permits the change operation of the user box password that is set to the public 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[5]**

FMT\_MTD.1[5] regulates the management of the user box password.

F.ADMIN permits the registration operation of the user box in the administrator mode, that is, the registration operation of the user box password that is set to the public user box. 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 register the user box password as a result of performing the restoration operation.

F.BOX permits the authenticated user the registration operation of the user box, that is, the registration operation of the user box password that is set to the public user box.

Accordingly, this functional requirement is satisfied.

- **FMT\_MTD.1[6]**

FMT\_MTD.1[6] 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[7]**

FMT\_MTD.1[7] regulates the management of the SNMP password, the User 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 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[8]**

FMT\_MTD.1[8] regulates the management of the Secure print password.

F.PRINT permits the registration of the secure print password to the user along with the registration of the secure print file.

Accordingly, this functional requirement is satisfied.

- **FMT\_MTD.1[9]**

FMT\_MTD.1[9] 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[10]**

FMT\_MTD.1[10] regulates the management of the user ID.

F.ADMIN permits the registration of the user ID in the administrator mode.

F.USER registers the user ID of the authenticated user, when the "External server authentication" is selected for the user authentication method and if the user who succeeds in the user authentication is not registered in the MFP. (This is equal to the registration to an external server.)

Accordingly, this functional requirement is satisfied.

- **FMT\_MTD.1[11]**

FMT\_MTD.1[11] regulates the management of the SNMP password.

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

Accordingly, this functional requirement is satisfied.

- **FMT\_MTD.1[12]**

FMT\_MTD.1[12] regulates the management of the administrator passphrase.

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

- Operation setting function of user authentication function
- 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 password
- User box password
- Secure Print password

It also corresponds to the modification function of the following TSF data.

- SNMP password
- User password
- User box password
- Secure print password
- User ID
- User attribute of the user box
- Panel auto log-off time
- 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 user attribute of the user box (User ID    Other User ID or Public)
  - Modification function of the administrator password
  - Registration/Modification function of the user box password
  - Registration function of the User ID
  - Registration/Modification function of the User password when "Machine authentication" is selected as the method of the user authentication
  - Modification function of the SNMP password (Privacy password and Authentication password )
  - Setting function of the Panel auto logoff time
  - 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 Public user box
  - Authentication function in the access to the secure print
  - User authentication function

F.ADMIN-SNMP offers security functions.

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

F.SERVICE offers the following security management functions.

- Modification function of the CE password
- Modification function of the administrator password
- Operational setting function of the maintenance function(through LAN)
- Initialization function of the SNMP password (Privacy password and Authentication password )
  - Initialization function(network setting)
- Stop function of the Enhanced Security function
  - HDD logical format function
  - HDD physical format function
  - Initialization function(network setting)

F.USER offers the following security management functions.

- Modification function of user's own user password when "Machine authentication" is selected as the method of the user authentication
- Automatic registration of the User ID for an unregistered user in MFP by the External server when the "External server authentication" is selected as the method of the user authentication

F.BOX offers the following security management functions.

- Modification function of the user attribute of the user box
  - Modification of a personal user box by the user (User ID    Public or Other User ID)
  - Modification of a public user box by the user who is permitted the use of the public user box (Public    User ID )
- Overwrite function of the default value of the user attribute of the user box
- Registration/Modification of the user box password

- Automatic registration of a personal user box by the stored job in the user box that specifies unregistered user box by the user.

F.PRINT offers the following security management functions.

- Registration of the Secure Print password

F.ADMIN and F.OVERWRITE-ALL offer 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.

F.USER recognizes the user who is authenticated by the user password as a user.

The user who is authenticated as a user by F.USER is recognized as a user similarly by succeeding to F.BOX and F.PRINT.

Accordingly, this functional requirement is satisfied.

● **FMT\_SMR.1[4]**

FMT\_SMR.1[4] 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 public user box.

Accordingly, this functional requirement is satisfied.

● **FMT\_SMR.1[5]**

FMT\_SMR.1[5] regulates the role as an external server.

F.USER recognized the reference to the user information as an external server when it is under the external server authentication.

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.USER definitely activates "User authentication function" of which performance is indispensable, before the use of various functions that can be performed only by the user 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 public 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.USER maintains the user authentication domain that is provided various functions permitted to operate only by the authenticated user, and it doesn't permit the interference by the unauthorized subject.

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 public 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.

- **FTA\_SSL.3**

FTA\_SSL.3 regulates the forced termination of a session to an administrator accessing from a panel.

F.ADMIN logs off automatically if the “panel auto log-off time” elapses from the last operation at the time of access from the panel by the administrator, and denies the access to the administrator authentication domain.

F.USER logs off automatically if the “panel auto log-off time” elapses from the last operation at the time of access from the panel by the administrator, and denies the access to the user authentication domain.

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 transmission address data file, the user ID, the user password, 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.

Administrator password authentication mechanism offered by F.ADMIN

CE authentication mechanism offered by F.SERVICE

Secure print password authentication mechanism offered by F.PRINT

User box password authentication mechanism offered by F.BOX

SNMP authentication mechanism offered by F.ADMIN-SNMP

User authentication mechanism offered by

HDD Lock password collation mechanism offered by F.ADMIN

Encryption Passphrase collation mechanism offered by F.ADMIN

It used the password composed from & an 8-digits and 92 kinds of character, & an

8-digits and 93 kinds of character, an 8-digits and 95 kinds of character, an 8-digits and 92 kinds of character, and & an 20-digits and 83 kinds of character. Among these, ~ locks the authentication function by the continuous three times of authentication failure by operating the authentication operation prohibition function.

The , and use the session information secretly in access via network. The secrets use the value of 1010 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.