bizhub C368/bizhub C308/bizhub C258/ bizhub C236DN/bizhub C230DN/bizhub C225DN/ ineo+ 368/ineo+ 308/ineo+ 258

Security Target

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

Version: 2.00

Issued on: May 24, 2016

Created by: KONICA MINOLTA, INC.

---- [Contents] ----

1 ST Introduction 6
1.1 ST Reference 6
1.2 TOE Reference 6
1.3 TOE Overview 6
1.3.1 TOE Type 6
1.3.2 Usage of the TOE 6
1.3.3 Necessary Hardware/Software for the TOE 8
1.3.4 TOE's Main Basic Functions and Main Security Functions 8
1.4 TOE description 9
1.4.1 Physical Scope of the TOE 9
1.4.2 Guidance 11
1.4.3 Identification of TOE Components 12
1.4.4 Logical Scope of the TOE 12
1.4.5 TOE User 16
1.4.6 Protected Assets 16
1.4.7 Glossary 17
1.4.8 User Box 21
2 Conformance Claims 22
2.1 CC Conformance Claim 22
2.2 PP Claim 22
2.3 Package Claim 22
2.3.1 SFR package reference 22
2.3.2 SFR Package functions 23
2.3.3 SFR Package attributes 24
2.4 PP Conformance rationale 24
2.4.1 Conformance Claim with TOE type of the PP 24
2.4.2 Conformance Claim with Security Problem and Security Objectives of the PP 24
2.4.3 Conformance Claim with Security requirement of the PP 25
3 Security Problem Definition 26
3.1 Threats agents 27
3.2 Threats to TOE Assets 27
3.3 Organizational Security Policies for the TOE 27
3.4 Assumptions 28
4 Security Objectives 29
4.1 Security Objectives for the TOE 29
4.2 Security Objectives for the IT environment 29
4.3 Security Objectives for the non-IT environment 30
4.4 Security Objectives rationale 31
5 Extended components definition (APE_ECD) 34
5.1 FPT_FDI_EXP Restricted forwarding of data to external interfaces 34
6 Security Requirements 36
6.1 Security functional requirements 36
6.1.1 Class FAU: Security audit 36
6.1.2 Class FCS: Cryptographic support 39
6.1.3 Class FDP: User data protection 40

6.1.4 Class FIA: Identification and authentication 46
6.1.5 Class FMT: Security management 49
6.1.6 Class FPT: Protection of the TSF 57
6.1.7 Class FTA: TOE access 58
6.1.8 Class FTP: Trusted path/channels 58
6.2 Security assurance requirements 59
6.3 Security requirements rationale 60
6.3.1 Common security requirements rationale 60
6.3.2 Security assurance requirements rationale 66
7 TOE Summary specification 68
7.1 F.AUDIT (Audit log function) 68
7.1.1 Audit log acquirement function 68
7.1.2 Audit Log Review Function 69
7.1.3 Audit storage function 69
7.1.4 Trusted time stamp function 69
7.2 F.HDD_ENCRYPTION (HDD Encryption function) 69
7.3 F.ACCESS_DOC (Accumulated documents access control function) 70
7.4 F.ACCESS_FUNC (User restriction control function) 71
7.5 F.RIP (Residual information deletion function) 73
7.5.1 Temporary Data Deletion Function 73
7.5.2 Data Complete Deletion Function 73
7.6 F.I&A (Identification and authentication function) 74
7.7 F.SEPARATE_EX_INTERFACE (External interface separation function) 76
7.8 F.SELF_TEST (Self-test function) 76
7.9 F.MANAGE (Security management function) 76
7.10 F.SECURE_LAN (Network communication protection function) 80

---- [List of Figures] ----

Figure 1-1 TOE's use environment 7
Figure 1-2 Physical scope of the TOE 10
Figure 1-3 Logical scope of the TOE 12

---- [List of Tables] ----

Table 1-1 Users 16
Table 1-2 User Data 16
Table 1-3 TSF Data 17
Table 1-4 TSF Data 17
Table 1-5 Glossary 18
Table 1-6 System User Box 21
Table 1-7 Function user box 21
Table 2-1 SFR Package functions 23
Table 2-2 SFR Package attributes 24
Table 3-1 Threats to User Data for the TOE 27
Table 3-2 Threats to TSF Data for the TOE 27
Table 3-3 Organizational Security Policies for the TOE 28
Table 3-4 Assumptions for the TOE 28
Table 4-1 Security Objectives for the TOE 29
Table 4-2 Security Objectives for the IT environment 29
Table 4-3 Security Objectives for the non-IT environment 30
Table 4-4 Completeness of Security Objectives 31
Table 4-5 Sufficiency of Security Objectives 32
Table 6-1 Audit data requirements 36
Table 6-2 Cryptographic key algorithm key size 39
Table 6-3 Cryptographic operations algorithm key size standards 40
Table 6-4 Common Access Control SFP 41
Table 6-5 PRT Access Control SFP 42
Table 6-6 SCN Access Control SFP 42
Table 6-7 CPY Access Control SFP 42
Table 6-8 FAX Access Control SFP 43
Table 6-9 DSR Access Control SFP 43
Table 6-10 TOE Function Access Control SFP 44
Table 6-11 Management of Object Security Attribute 50
Table 6-12 Management of Subject Security Attribute 51
Table 6-13 Management of Subject Attribute 52
Table 6-14 Management of Object Attribute 52
Table 6-15 Characteristics Static Attribute Initialization 53
Table 6-16 Characteristics Static Attribute Initialization 54
Table 6-17 Operation of TSF Data 55
Table 6-18 Operation of TSF Data 56
Table 6-19 list of management functions 56
Table 6-20 IEEE 2600.2 Security Assurance Requirements 59
Table 6-21 Completeness of security requirements 60
Table 6-22 Sufficiency of security requirements 61

Table 6-23 The dependencies of security requirements 65
Table 7-1 Names and identifiers of TOE Security Functions 68
Table 7-2 Audit Log 68
Table 7-3 Encryption Algorithm in HDD Encryption function 70
Table 7-4 Operation of document in the System user box 70
Table 7-5 Details of Operation of document in the System user box 70
Table 7-6 Operation for documents in the function user box 70
Table 7-7 Details of Operation for documents in the function user box 71
Table 7-8 Operation Settings of Overwrite Deletion function of Temporary data 73
Table 7-9 Operation settings of Data Complete Deletion Function 73
Table 7-10 Authentication method 74
Table 7-11 Password and Quality 75
Table 7-12 Process at the time of authentication failure 75
Table 7-13 Termination of interactive session 75
Table 7-14 Management Function 77
Table 7-15 Secure Print Password management function 80
Table 7-16 Encryption Communication provided by the TOE 80

1 ST Introduction

1.1 ST Reference

- ST Title	:	bizhub C368/bizhub C308/bizhub C258/ bizhub C236DN/bizhub C230DN/bizhub C225DN/ ineo+ 368/ineo+ 308/ineo+ 258 Security Target
- ST Version	:	2.00
- Created on	:	May 24, 2016
- Created by	:	KONICA MINOLTA, INC.

1.2 TOE Reference

- TOE Name	:	bizhub C368/bizhub C308/bizhub C258/ bizhub C236DN/bizhub C230DN/bizhub C225DN/ ineo+ 368/ineo+ 308/ineo+ 258
- TOE Version	:	G00-83
- Created by	:	KONICA MINOLTA, INC.

1.3 TOE Overview

The TOE is the MFP used in the network environment (LAN), and has the function to accumulate documents in addition to copy, scan, print and FAX functions. The connection of FAX kit (option) is necessary to use FAX function.

1.3.1 TOE Type

The TOE is the MFP used in the network environment (LAN).

1.3.2 Usage of the TOE

TOE's use environment is shown below, and the usage for the TOE is described. The hardware and software necessary for using the TOE, which are not the TOE, is described in 1.3.3.

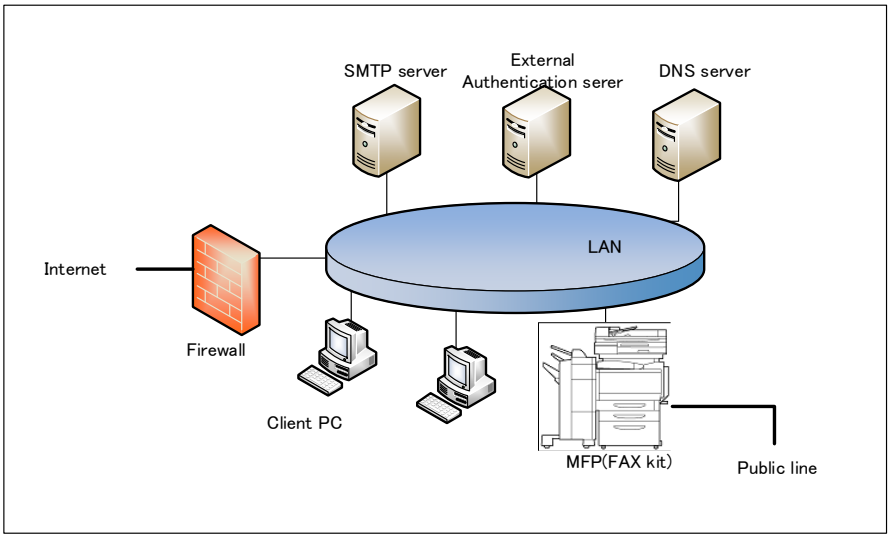

Figure 1-1 TOE's use environment

The TOE is used by connecting LAN and public line, as shown in Figure 1-1. The User can operate the TOE by communicating through the LAN or the operation panel with which the TOE is equipped. The following explain about the MFP, which is the TOE, and the hardware and software, which are not the TOE.

(1) MFP

This is the TOE. MFP is connected to the intra-office LAN. The user can perform the following from the operation panel.

- MFP's various settings
- Paper documents' Copy, Fax TX, Accumulation as electronic documents, Network TX
- Accumulated documents' Print, Fax TX, Network TX, Deletion

(2) FAX kit

Necessary option for using fax function.

(3) LAN

Network used for the TOE setup environment.

(4) Public line

Telephone line for transmitting to external fax.

(5) Firewall

Device for protecting against the network attacks to intra-office LAN from the internet.

(6) Client PC

By connecting to the LAN, this works as the client of the TOE. The user can access MFP from the client PC and operate the following by installing the Web browser, the printer driver, and the device management software tool for administrator etc. in the client PC.

- MFP's various settings
- Document Operation

- Accumulation, Print of electronic documents

(7) SMTP server
Server used for sending the electronic documents in the TOE by e-mail.

(8) External Authentication server
Server to identify and authenticate TOE users. This is used only when external server authentication method is used. Kerberos authentication is used in the external server authentication method.

(9) DNS server
Server for converting domain name to IP address

1.3.3 Necessary Hardware/Software for the TOE

The following are the hardware and software necessary for using the TOE.

Hardware /Software	Used version for evaluation
FAX kit	FK-514 (KONICA MINOLTA)
Web Browser	Microsoft Internet Explorer 11
Printer Driver	KONICA MINOLTA C368 Series PCL Ver. 3.1.4.0 PS Ver. 3.1.4.0 XPS Ver. 3.1.4.0
Device Management Software tool for Administrator	KONICA MINOLTA Data Administrator with Device Set-Up and Utilities Ver.1.0.06000 KONICA MINOLTA Data Administrator Ver. 4.1.34000
External Authentication Server	Active Directory installed in Microsoft Windows Server 2008 R2 Standard Service Pack1
DNS Server	Microsoft Windows Server 2008 R2 Standard Service Pack1

1.3.4 TOE's Main Basic Functions and Main Security Functions

TOE's main basic functions are as follows.

(1) Print
Function to print the print data.

(2) Scan
Function to generate a document file by scanning paper documents.

(3) Copy
Function to copy scanned image by scanning paper documents.

(4) FAX
Function to send the scanned paper documents to the external FAX. Function to receive documents from the external FAX.

(5) Document storage and retrieval function
Function to accumulate documents in the TOE and retrieve the accumulated documents.

(6) Shared-medium interface function
Function to operate the TOE remotely from the Client PC by TOE users.

TOE's main security functions are as follows.

(1) Identification and authentication function
Function to identify and authenticate TOE users

(2) Accumulated documents access control function
Function to control the operation of accumulated documents.

(3) User restriction control function
Function to control the operation of TOE functions and to control the operation to the documents other than the accumulated documents included in the performing jobs.

(4) HDD encryption function
Function to encrypt recorded data to HDD.

(5) Audit log function
Function to record the log of events related to TOE usage and security as the audit log and to refer to it.

(6) Residual information deletion function
Function to disable the reuse of the deleted documents, temporary documents or its fragmented files in the TOE.

(7) Network communication protection function
Function to prevent the disclosure of information caused by wiretapping on the network when using the LAN.

(8) Self-test function
Function to verify that HDD encryption function, encryption passphrase and TSF executable code are normal when starting MFP.

(9) Security management function
Function to control the operation to TSF data and the behavior of security function.

(10) External interface separation function
Function to disable the direct forwarding of the input from the external interface, including USB interface, to Shared-medium Interface, and also to prevent the intrusion to the LAN from the telephone line.

1.4 TOE description

This paragraph explains the overview of the physical scope of the TOE, the TOE user's definition, the logical scope of the TOE and the protected assets.

1.4.1 Physical Scope of the TOE

The TOE, as shown in Figure 1-2, is the MFP composed of main/sub power, operation panel, scanner unit, MFP controller unit, printer unit and HDD.

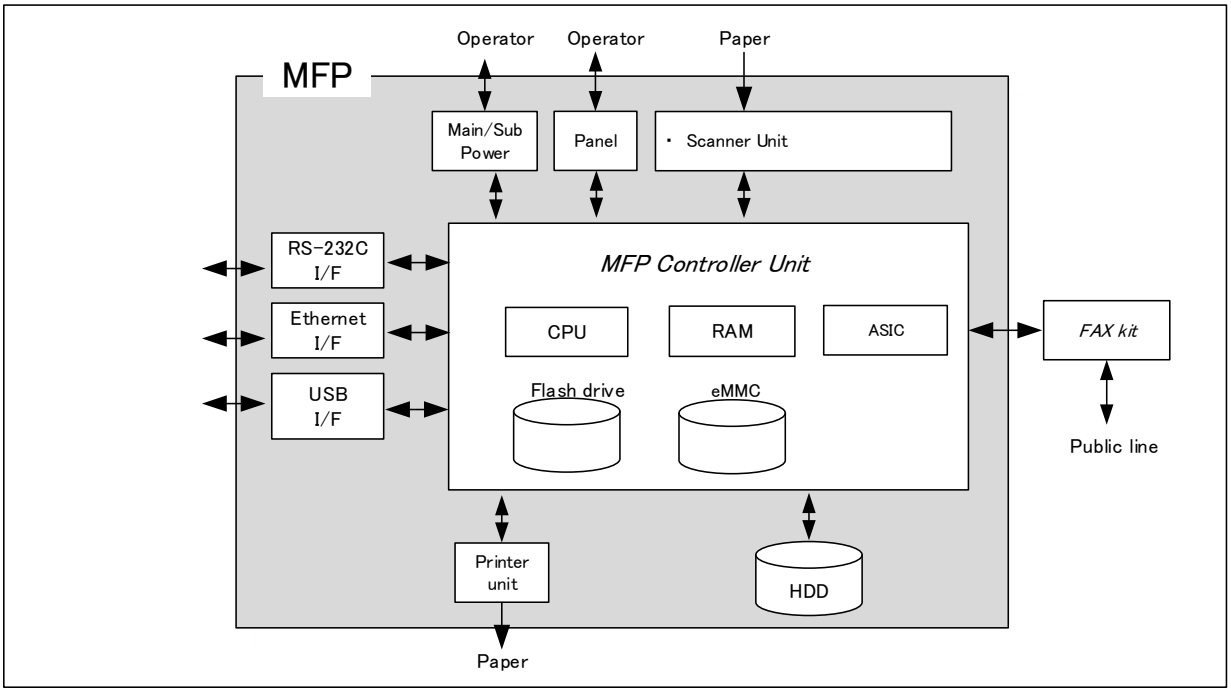

Figure 1-2 Physical scope of the TOE

(1) Main/sub power supply
Power switches for activating MFP.

(2) Operation Panel
An exclusive control device for the operation of MFP, equipped with a touch panel of a liquid crystal monitor, numeric keypad[1], start key, stop key, screen switch key, etc.

(3) Scanner unit
A device that scans images and photos from paper and converts them into digital data.

(4) MFP Controller unit
A device that controls MFP.

(5) CPU
Central processing unit.

(6) RAM
A volatile memory used as the working area.

(7) ASIC
An integrated circuit for specific applications which implements an HDD encryption functions for enciphering the image data written in HDD.

(8) Flash drive

[1] Numeric keypad is displayed on the touch panel. Hard numeric keypad is the option (Not the TOE).

A nonvolatile memory that stores TSF data that decides MFP action.

(9) eMMC

A storage medium that stores the object code of the "MFP Control Software." Additionally, it stores the message data expressed in each country's language to display the response to access through the operation panel and network, and various settings that the MFP needs.

(10) Printer unit

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

(11) HDD

A hard disk drive of 250GB in capacity. This is used not only for storing electronic documents as files but also for working area. The HDD is not the removable nonvolatile storage device on this TOE.

(12) RS-232C I/F

Interface which is usable for the serial connection using D-sub 9-pin connectors. The maintenance function can be used through this interface at the time of a breakdown. It is possible to use the remote diagnostic function (described later) by connecting with the public line via a modem.

(13) Ethernet I/F

Interface which supports 10BASE-T, 100BASE-TX, and Gigabit Ethernet.

(14) USB I/F

Used for rewriting the firmware according to the guidance.

(15) FAX kit

A device that is used for communications for FAX-data transmission and remote diagnostic via the public line. This is not included in the TOE.

1.4.2 Guidance

There are English and Japanese versions of TOE guidance, and they are distributed depending on sales areas. The following show the list of guidance.

Name	Ver.
bizhub C368/C308/C258 User's Guide (Japanese)	1.00
bizhub C368/C308/C258 User's Guide Security Functions (Japanese)	1.01
bizhub C368/C308/C258 User's Guide	1.00
bizhub C368/C308/C258 User's Guide [Security Operations]	1.01
bizhub C368/C308/C258/C236DN/C230DN/C225DN User's Guide [Security Operations][2]	1.01

[2] Guidance for Korean model: Guidance is composed by User's Guide and User's Guide [Security Operations]. This guidance and bizhub C368/C308/C258 User's Guide are corresponding to the Korean model.

ineo+ 368/308/258 User's Guide	1.00
ineo+ 368/308/258 User's Guide [Security Operations]	1.01

1.4.3 Identification of TOE Components

Each of the MFP, MFP board, firmware, and eMMC board which compose the TOE, has its own identification. The relation between each identification is as follows.

MFP	MFP board	eMMC board	Firmware
bizhub C368	A7PUH020-05	A7AHH02D-00	A7PU0Y0-F000-G00-83
bizhub C308			
bizhub C258			
bizhub C236DN			
bizhub C230DN			
bizhub C225DN			
ineo+ 368			
ineo+ 308			
ineo+ 258			

1.4.4 Logical Scope of the TOE

TOE security functions and the basic functions are described below.

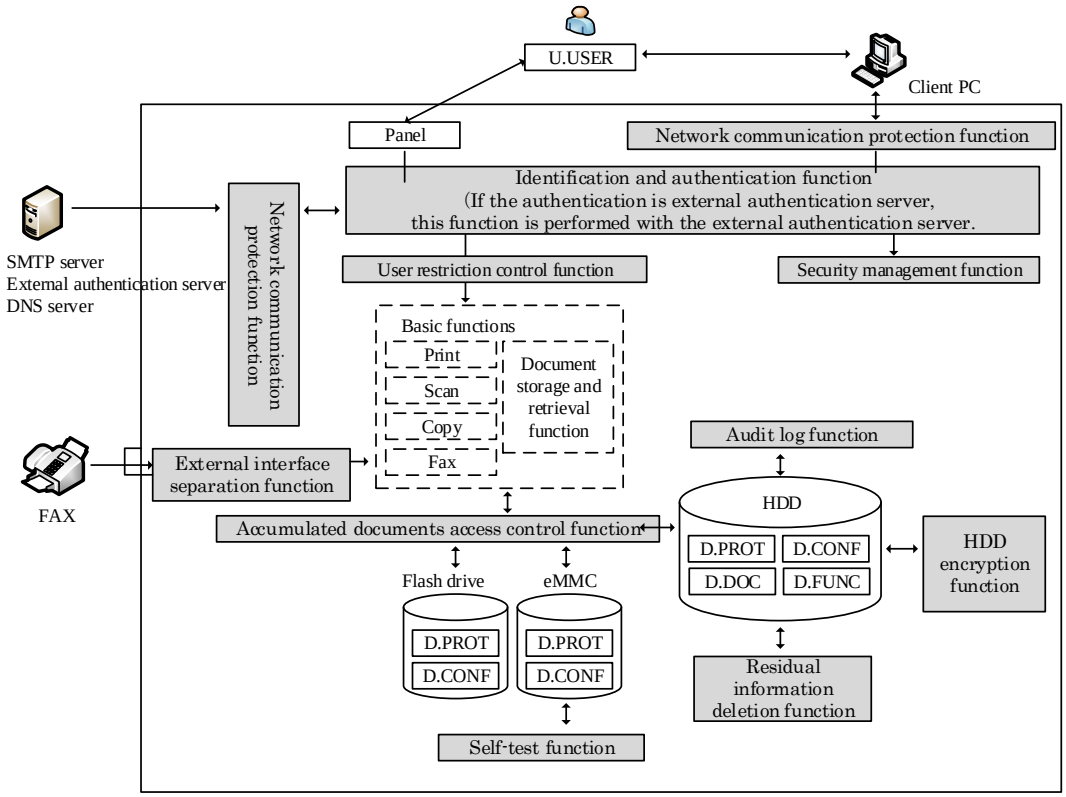

Figure 1-3 Logical scope of the TOE

1.4.4.1 Basic Functions

TOE basic functions are described below.

(1) Print

This function prints the print data received via LAN from a client PC.

(2) Scan

This function scans a document (paper) by user's operation from operation panel and generates a document file.

(3) Copy

This function scans a document (paper) by user's operation from operation panel and copies a scanned image.

(4) FAX

This function scans a paper document and sends it to external fax (FAX TX function), and receives the document from external fax (FAX RX function).

The TOE can accumulate the documents and also can send the accumulated documents in the TOE by Fax. Documents accumulated in the TOE that can be sent by Fax is called Fax TX print. In addition, documents received by Fax are accumulated in the TOE and can be printed and deleted.

- Fax TX function
  Function to send a paper document and Fax TX print to the external fax device from the telephone line. The paper document is scanned by the operation on the panel and performs Fax TX. Fax TX print is operated from the operation panel and performs Fax TX.
- Fax RX function
  Function to receive documents through the telephone line from the external fax.

(5) Document storage and retrieval function

This function accumulates documents in the TOE and retrieves the accumulated documents.

(6) Shared-medium interface function

This function operates the TOE remotely from the Client PC by TOE users. Along with the guidance, Web browser or application, etc. is installed and connected with the TOE through LAN.

1.4.4.2 Security Functions

TOE security functions are described below.

(1) Identification and authentication function

This function verifies whether a person who uses the TOE is the authorized user of the TOE or not by user ID and password. If it was confirmed to be the authorized user of the TOE, this function permits the use of the TOE. There are machine authentication and external server authentication as the methods to verify, and it is authenticated by the method which was set by administrator beforehand.

This function includes the function to display the input password on the operation panel with dummy characters. Moreover, it includes the authentication lock function when the continuous number of authentication failures reaches to the setting value, and the function to register only passwords that satisfy the conditions, like minimum character of password, set by administrator for keeping the password quality.

(2) Accumulated documents access control function

This function permits operation of accumulated documents for authorized user of the TOE who was authenticated by identification and authentication function, based on the authority given to the user's role or the attributes of user and the attributes of documents.

(3) User restriction control function

This function permits the operation of print, scan, copy, fax, document storage and retrieval function, and shared-medium interface function for authorized user of the TOE who was authenticated by identification and authentication function, based on the operation authority given to the user's role or each user. Also, this function takes control of the operation of documents other than accumulated documents included in executing jobs.

(4) HDD encryption function

This function encrypts data saved in the HDD for protecting against unauthorized disclosure.

(5) Audit log function

This function records logs of the events related to the TOE use and security (hereinafter, referred to as “audit event”) with date and time information as the audit log, and provides the recorded audit log in the auditable form. Audit log is stored in the HDD of the TOE, but if the storage area becomes full, accepting jobs is suspended (Audit log is not stored.) or oldest audit record stored is overwritten according to administrator’s settings. Moreover, recorded audit log is permitted to read and delete only by administrator.

(6) Residual information deletion function

This function makes residual information non-reusable by overwriting the deleted documents, temporary documents, or their parts in the TOE with special data.

(7) Network communication protection function

This function prevents the disclosure of information by wiretapping on a network when using the LAN. This function encrypts the communication data between client

PC and MFP, and between external authentication server, DNS server, SMTP server, and MFP.

(8) Self-test function

This function verifies that HDD encryption function, encryption passphrase, and TSF executable code are normal when starting MFP.

(9) Security management function

This function controls the operation to TSF data and the behavior of security function for authorized user of the TOE who was authenticated by identification and authentication function based on the authority given to the user's role.

(10) External interface separation function

This function prevents transferring the input from external interfaces, including USB interface, to Shared-medium Interface as it is, and prevents the intrusion to LAN from telephone line. Regarding the telephone line, this function prevents intrusion from the telephone line by limiting the input information only to FAX RX and Remote diagnostic function, and prevents the intrusion to LAN from the telephone line by prohibiting the transfer of received fax.

1.4.4.3 Restriction

Prohibited functions and unusable functions are described below.

- FTP TX, SMB TX, WebDAV TX, IP address FAX, Internet FAX, PC-FAX RX
- Bulletin Board User box, etc., which are not listed in the ST
- SNMP function
- DPWS setting
- LPD setting
- RAW print
- Print function with USB local connection
- External memory (Print, Save document, Copy)
- Print function other than Secure Print, ID & Print, and Encrypted PDF (By this restriction, it is stored as print authentication and print document even if print is requested with normal print settings.)

1.4.5 TOE User

TOE users (U.USER) are classified as follows.

Table 1-1 Users

Designation			Definition
U.USER (Authorized user)			Any authorized User.
	U.NORMAL (Public user)		A User who is authorized to perform User Document Data processing functions of the TOE.
	U.ADMINISTRATOR (Administrator)	U.BUILTIN_ADMINISTRATOR (Built-in administrator)	A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP.
		U.USER_ADMINISTRATOR (User administrator)	

*Refer to 1.4.7 Glossary about U.BUILTIN_ADMINISTRATOR and U.USER_ ADMINISTRATOR.

1.4.6 Protected Assets

Protected assets are User Data, TSF Data and Functions.

1.4.6.1 User Data

User Data are generated by or for the authorized users, which do not have any effect on the operations of TOE security functions. User data are classified as follows.

Table 1-2 User Data

Designation	Definition
D.DOC	User Document Data consists of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually stored data created by the hardcopy device while processing an original document and printed hardcopy output.
D.FUNC	User Function Data are the information about a user's document or job to be processed by the TOE.

1.4.6.2 TSF Data

TSF Data are data generated by or generating for the TOE, which affect TOE operations. TSF Data are classified as follows.

Table 1-3 TSF Data

Designation	Definition
D.PROT	TSF Protected Data are assets for which alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE, but for which disclosure is acceptable.
D.CONF	TSF Confidential Data are assets for which either disclosure or alteration by a User who is neither an Administrator nor the owner of the data would have an effect on the operational security of the TOE.

TSF Data covered in this TOE are as follows.

Table 1-4 TSF Data

Designation	Definition
D.PROT	Auto reset time Auto logout time Authentication Failure Frequency Threshold Password mismatch frequency threshold Data which relates to access control (Authentication failure frequency, Password mismatch frequency, etc.) External server authentication setting data Operation prohibition release time of Administrator authentication Time information Network settings (IP address of SMTP server, Port No., etc., MFP IP address, etc.) TX address settings (address of e-mail TX, etc.) Password Policy Settings which relate to transfer of RX FAX User ID Permission Role Allocation Role Role
D.CONF	Login password Encryption passphrase sBOX PASSWORD DOC PASSWORD Audit log

1.4.6.3 Functions

Functions shown in 2.3.2 SFR Package functions.

1.4.7 Glossary

The meanings of terms used in this ST are defined.

Table 1-5 Glossary

Designation	Definition
Allocation Role	Attributes related to a user. Refer when MFP function is executed.
Box Type	Types of user box; Secure print user box, Memory RX user box, Password Encrypted PDF user box, ID & Print user box, Annotation user box.
Copy Role	Role which can perform a copy.
Data Administrator	Application software to perform administrator settings from client PC.
Data Administrator with Device Set-Up and Utilities	Device management software for administrator corresponding to multiple MFP. Possible to activate Data Administrator which is plug-in software.
DSR Role	Role which can store data to HDD, can read out stored data in HDD, and can edit.
Fax Role	Role which can perform a fax function.
FTP TX	Function which uploads to FTP server by converting scanned data to the available file on the computer.
HDD data overwrite deletion function	Function to overwrite and delete the data on HDD.
Operation settings of HDD data overwrite deletion function	Function which sets the deletion methods which are used for HDD data overwrite deletion function.
Permission Role	Attributes related to MFP function.
Print Role	Role which can perform a print from a client PC.
Role	Role of U.USER. There are U.NORMAL and U.ADMINISTRATOR. Moreover, U.ADMINISTRATOR is divided into U.BUILTIN_ADMINISTRATOR and U.USER_ADMINISTRATOR.
Scan Role	Role which can perform a scan.
SMB TX	Function which transmits to a computer and a public folder of server by converting scanned data to the available file on the computer.
User Role	Necessary role when print, scan, copy, FAX and store of files are performed.
U.BUILTIN_ADMINISTRATOR (Built-in administrator)	Role of U.USER Role given only to the administrator implemented in the TOE beforehand (built-in administrator).
U.USER_ADMINISTRATOR (User administrator)	Role of U.USER Role given by the U.ADMINISTRATOR Able to operate as this role by being succeed at the login from the interface for U.USER_ADMINISTRATOR. Same as U.BUILTIN_ADMINISTRATOR, excepting the availability of addition and deletion of the role, and the handling at the time of failure.
Web Connection	Function to change MFP settings and confirm status by using Web

	browser of the computer on the network.
WebDAV TX	Function which uploads to WebDAV server by converting scanned data to the available file on the computer.
Remote diagnostic function	MFP's equipment information, such as operating state and the number of printed sheets, is managed by making use of the connection by a modem through a port of FAX public line or by E-mail to communicate with the support center of MFP produced by KONICA MINOLTA, INC. In addition, if necessary, appropriate services (shipment of additional toner packages, account claim, dispatch of service engineers due to the failure diagnosis, etc.) are provided.
Auto Reset	Function which logs out automatically when there is not access for a period of set time during logging-in.
Auto Reset Time	Setup time by administrator. It logs out automatically after this time passes. Operation from the panel is an object.
Job	Document processing task which is sent to hard copy device. Single processing task can process more than one document.
Enhanced security settings	Function to set the setting which is related to the behavior of the security function, collectively to the secure values and maintain it. When this function is activated, the use of the update function of the TOE through the network, the initializing function of the network setting, and the setting change by remote diagnostic function are prohibited, or alert screen is displayed when it is used. The alert screen is displayed when the setting value is changed. Then, Enhanced security settings become invalid if the setting value is changed (only administrator can do).
Secure Print (SECURITY DOCUMENT)	The document which saved in the TOE with the password specified from the client PC side.
Secure Print Password (DOC PASSWORD)	Password which is set in secure print.
Password mismatch frequency threshold	Threshold that administrator sets. The access to the user box is prohibited when number of continuous mismatch of user box password and input password reached this threshold. The access to the secure print is prohibited when the number of continuous mismatch of secure print password and input password reached this threshold.
Annotation User Box	User box that is managed by the administrator who sets up the processing (date, numbering). When retrieving (print, send) the saved document from the user box, setup process is added.
Print job input function	Function that the TOE receives the User ID, the login password and the print data which are sent from client PC. Only when the identification and authentication of User ID and login password succeeded, the print data are received.
User box	Directory to store documents.

	Stored documents include the accumulated documents, and documents included in the executing job. User who can save documents and operate, is different according to a user box.
User box password (BOX PASSWORD)	Password given to user box. Password which only U.ADMINISTRATOR can change is shown as sBOX PASSWORD.
User ID (User ID)	Identification that is given to a user. The TOE specifies a user by that identification. At the external server authentication, this is composed of User ID + External server ID.
Temporary suspension and Release of User ID	Temporary suspension: to temporarily suspend the login of the considered User ID. Release: to release the temporary suspension.
User management function	Function to perform registration / deletion of user and addition / deletion / change of the authority.
User authentication function	Function to authenticate TOE users. There are two types. Machine authentication (INTERNALLY AUTHENTICATION) and External server authentication (EXTERNALLY AUTHENTICATION). U.BUILTIN_ADMINISTRATOR is authenticated only by Machine Authentication.
Management function of User Authentication	Function which sets authentication methods (MFP authentication / External server authentication).
Login	To identify and authenticate on the TOE by user ID and login password.
Login Password (LOGIN PASSWORD)	Password for logging in the TOE.
Encryption passphrase	Data which is used for generating encryption key which is used with HDD encryption. The TOE generates encryption key by using encryption passphrase.
External server authentication setting data	Setting data related to the external authentication server. (Including domain name which external server belongs to)
Audit log management function	Function which sets the operation when audit log was full.
Audit log function	Function to obtain audit logs.
Operation prohibition release time of Administrator authentication	Time until a lock is released, when the number of continuous authentication failure is reached to the settings and the the authentication of U.BUILTIN_ADMINISTRATOR is locked.
Bulletin Board User Box	User box which accumulates documents for the polling TX (Fax TX with the request from others.
Trust Channel Function	Function to protect transmitting data via LAN by encrypting.
Trust Channel Management Function	Function to perform Trust Channel function, and to manage SSL/TLS server certification and cryptographic method.
Residual information deletion function	Function to delete the data on HDD by HDD data overwrite deletion function.
Time information	Information of time. When any event occurred, the time

	information is recorded on audit log.
Auto logout time	Time set by administrator. Automatically logs out after the setting time. Web Connection is an object.
Session Auto terminate function	Function to terminate session automatically. Terminate the session automatically when no operation is performed for a certain period of time on each of Operation panel, Web Connection, and Data Administrator.
ID & Print function (AUTH PRINT)	Function to save the document which has user name and password which is sent from PC on the network as the directed print document.
Authentication Failure Frequency Threshold	Threshold that administrator sets. Authentication function is locked when number of continuous authentication failure reached this threshold.
Account Password	Password that is managed by the administrator who input at the initial authentication for external authentication method.
Accumulated document	Documents for storing and retrieving (the object of operation by F.DSR)

1.4.8 User Box

This paragraph describes the user box that the TOE provides. The TOE provides the following types of User box. (This is categorized based on the characteristic of user box, but this does not necessarily match to the display on the operation panel. Also, Bulletin Board User Box, etc., exists other than this, but except the types of user box described here, cannot be used.)

Table 1-6 System User Box

User box Type	Description
Secure Print user box	User box that stores the secure print.
Memory RX user box	User box that stores FAX RX document (Accumulated document). When Memory RX setting is ON, RX document is saved in the Memory RX user box. U.ADMINISTRATOR performs the Memory RX setting.
Password Encrypted PDF used box	User box that stores the encrypted PDF (PDF file that requires inputting password when it opened.) By specifying the document and inputting the password, the document can be printed.
ID & Print user box	User box that stores documents by ID & Print function

Table 1-7 Function user box

User box Type	Description
Annotation user box	User box that is managed by the administrator who can print and send the stored document data (accumulated document) by the addition of date/ time and image of filing number.

2 Conformance Claims

2.1 CC Conformance Claim

This ST conforms to the following Common Criteria (hereinafter referred to as "CC").

CC version	:	Version 3.1 Release 4
CC conformance	:	CC Part 2 extended, CC Part 3 conformant
Assurance level	:	EAL2 augmented by ALC_FLR.2

2.2 PP Claim

This ST conforms to the following PP.

PP name/identification	:	U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std 2600.2™-2009)
Version	:	1.0

Notes) This PP conforms to "IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008, Operational Environment B", published in Common Criteria Portal, and also satisfies "CCEVS Policy Letter #20".

2.3 Package Claim

This ST conforms to the following SFR Packages.

-2600.2-PRT	Conformant
-2600.2-SCN	Conformant
-2600.2-CPY	Conformant
-2600.2-FAX	Conformant
-2600.2-DSR	Conformant
-2600.2-SMI	Conformant

2.3.1 SFR package reference

Title	:	2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B
Package version	:	1.0
Date	:	March 2009

Title	:	2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B

Package version : 1.0
Date : March 2009

Title : 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B
Package version : 1.0
Date : March 2009

Title : 2600.2-FAX, SFR Package for Hardcopy Device Fax Functions, Operational Environment B
Package version : 1.0
Date : March 2009

Title : 2600.2-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment B
Package version : 1.0
Date : March 2009

Title : 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B
Package version : 1.0
Date : March 2009

2.3.2 SFR Package functions

Functions perform processing, storage, and transmission of data that may be present in HCD products. The functions that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in Table 2-1.

Table 2-1 SFR Package functions

Designation	Definition
F.PRT	Printing: a function in which electronic document input is converted to physical document output
F.SCN	Scanning: a function in which physical document input is converted to electronic document output
F.CPY	Copying: a function in which physical document input is duplicated to physical document output
F.FAX	Faxing: a function in which physical document input is converted to a telephone-based document facsimile (fax) transmission, and a function in which a telephone-based document facsimile (fax) reception is converted to physical document output
F.DSR	Document storage and retrieval: a function in which a document is stored during one job and retrieved during one or more subsequent jobs
F.SMI	Shared-medium interface: a function that transmits or receives User Data or TSF Data over a communications medium which, in conventional practice, is or can be simultaneously accessed by multiple users, such as wired network media and most radio-frequency wireless media

2.3.3 SFR Package attributes

When a function is performing processing, storage, or transmission of data, the identity of the function is associated with that particular data as a security attribute. This attribute in the TOE model makes it possible to distinguish differences in Security Functional Requirements that depend on the function being performed. The attributes that are allowed, but not required in any particular conforming Security Target or Protection Profile, are listed in Table 2-2.

Table 2-2 SFR Package attributes

Designation	Definition
+PRT	Indicates data that are associated with a print job.
+SCN	Indicates data that are associated with a scan job.
+CPY	Indicates data that are associated with a copy job.
+FAXIN	Indicates data that are associated with an inbound (received) fax job.
+FAXOUT	Indicates data that are associated with an outbound (sent) fax job.
+DSR	Indicates data that are associated with a document storage and retrieval job.
+SMI	Indicates data that are transmitted or received over a shared-medium interface.

2.4 PP Conformance rationale

2.4.1 Conformance Claim with TOE type of the PP

The product type that the PP intends is Hard Copy Device (Hereinafter referred to as "HCD"). The HCD is a product used for converting hard copy document to digital form (SCAN) or for converting digital document to hard copy form (PRINT) or for transmitting hard copy document through the telephone line (FAX), or for generating a copy of hard copy document (COPY).

The HCD is implemented by many different configurations depending on objectives, and in order to extend a function, there are some which have added hard disk drive, other non-volatile storage system or document server function, etc.

This TOE type is the MFP. The MFP have devices that the HCD has including additional devices and functions that the HCD has are installed. Therefore, this TOE type is consistent with the PP's TOE type.

2.4.2 Conformance Claim with Security Problem and Security Objectives of the PP

Addition of P.HDD.CRYPTO and O.HDD.CRYPTO

P.HDD.CRYPTO requests to encrypt the data recorded in HDD. This does not give restriction relating to operational environment, but restricts the TOE. O.HDD.CRYPTO is corresponding to added OSP and this also does not give restriction relating to operational environment, but restricts the TOE. Therefore, the ST imposes restriction on the TOE more than the PP and imposes on TOE's operational environment equivalent to the PP. This satisfies the conditions that are equivalent or more restrictive to the PP.

2.4.3 Conformance Claim with Security requirement of the PP

The SFRs of this TOE consist of Common Security Functional Requirements, 2600.2-PRT, 2600.2-SCN, 2600.2-CPY, 2600.2-FAX, 2600.2-DSR and 2600.2SMI.

Common Security Functional Requirements are mandatory SFRs specified by the PP and 2600.2-PRT, 2600.2-SCN, 2600.2-CPY, 2600.2-FAX, 2600.2-DSR, and 2600.2-SMI are selected from SFR Packages specified by the PP.

Security requirements of this ST include the part that is added and fleshed out to security requirements of the PP, but this is consistent with the PP. The following describes the part that is added and fleshed out, and the rationale that those are consistent with the PP.

Common Access Control SFP

The PP defines access control relating to Delete and Read of D.DOC that has attributes of +FAXIN, and Modify and Delete of D.FUNC, but anybody can cancel FAX communication that the TOE is receiving, without restriction. And so, D.DOC and D.FUNC under receiving are deleted. However, this is not the process to intend to Delete of D.DOC and D.FUNC and this is the Delete associated with the cancel of transmission. Other than it is recorded as log, this does not undermine the requirement of the PP, since this is saved in the user box after receiving and protected by becoming the object of DSR Access Control SFP. Also, it cannot Modify D.FUNC of FAX under receiving. This is the access control more restricted than PP.

The TOE defines access control relating to Modify of D.DOC that has attributes of +SCN and +FAXOUT. This is not defined in the PP, but this restricts deletion with page unit to U.NORMAL that is the owner of D.DOC. Access control relating to Delete is defined in the PP, but the TOE provides Delete function with page unit in addition to same access control with the PP. However, that operation is restricted to owner of D.DOC and this does not relax the restriction of access control SFP of the PP.

Addition of FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4(1), FAU_STG.4(2)

This TOE adds FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.4(1) and FAU_STG.4(2) in accordance with the PP APPLICATION NOTE5 and PP APPLICATION NOTE7 to maintain and manage the audit log.

Addition of FCS_CKM.1, FCS_COP.1, FIA_SOS.1(2)

This TOE adds O.HDD.CRYPTO as Objectives, and with that, FCS_CKM.1, FCS_COP.1 and FIA_SOS.1(2) are added, but this does not mean to change the contents of security requirements specified by the PP.

Conformance of FDP_ACF.1(a)

FDP_ACF.1 (a) of the PP requires access control SFP that permits access only to his/her own documents and to his/her own function data. This TOE performs access control based on the security attributes of D.DOC and D.FUNC, and other than that, D.DOC and D.FUNC that are saved in the TOE is stored in the user box under protected directory and those are protected by the access control of user box. Documents accumulated in the user box protected by

password is protected by the user box password, and the user (administrator in this TOE) who manages user box password is positioned as the owner of D.DOC and D.FUNC in the user box and it performs access control.

Addition of FIA_AFL.1, FIA_SOS.1(1), FIA_UAU.7

Machine authentication is the function that this TOE implements. In accordance with the PP APPLICATION NOTE 38, FIA_AFL.1, FIA_SOS.1(1) and FIA_UAU.7 are added.

Addition of FMT_MOF.1

The TOE has the function to enable and disable Enhanced Security Setting. The TOE requires operating in the state of enabled Enhanced Security Setting by the guidance, and FMT_MOF.1 restricts the change of Enhanced Security Setting only to U.ADMINISTRATOR and prevents from unauthorized change of Enhanced Security setting. This is not the change of content of security requirement specified by the PP.

FMT_MOF.1 restricts the management function about FTP_ITC.1 and the management of User Authentication function only to U.ADMINISTRATOR and prevents from unauthorized execution of management function. This is not the change of content of security requirement specified by the PP.

The management of behavior of “HDD data overwrite deletion function” manages the behavior of the overwrite deletion function to protect the residual information and this is not the change of content of security requirement specified by the PP.

The management of behavior of audit function manages the operation at the time of audit log full and this is not the change of content of security requirement specified by the PP.

Relation between FMT_MSA.1(a), FMT_MSA.1(b) and Objectives

The relationship between these functional requirements and objectives are different from PP, but this does not change the contents of security requirements specified by the PP. This is because disclosure and alteration of security attribute based on TSF data, such as attribute of user box, produces the same result with disclosure and alteration of TSF data itself and management of a security attribute has the same purpose and effect as protection of TSF data.

Relation between FMT_MTD.1 and Objectives

U.ADMINISTRATOR who has the administrator role of TOE is divided into U.BUILTIN_ADMINISTRATOR and U.USER_ADMINISTRATOR. U.BUILTIN_ADMINISTRATOR is the role given only to the administrator implemented in the TOE beforehand (built-in administrator). U.USER_ADMINISTRATOR is the role given by U.BUILTINT_ADMINISTRATOR and U.USER_ADMINISTRATOR. Both are the administrator role of the TOE and do not conflict with the separation of the authentication of U.ADMINISTRASTOR and U.NORMAL. This does not change the contents of security requirements specified by the PP.

3 Security Problem Definition

3.1 Threats agents

This security problem definition addresses threats posed by four categories of threat agents:

a) Persons who are not permitted to use the TOE who may attempt to use the TOE.

b) Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.

c) Persons who are authorized to use the TOE who may attempt to access data in ways for which they are not authorized.

d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

The threats and policies defined in this Protection Profile address the threats posed by these threat agents.

3.2 Threats to TOE Assets

This section describes threats to assets described in clause in 1.4.6.

Table 3-1 Threats to User Data for the TOE

Threat	Affected asset	Description
T.DOC.DIS	D.DOC	User Document Data may be disclosed to unauthorized persons
T.DOC.ALT	D.DOC	User Document Data may be altered by unauthorized persons
T.FUNC.ALT	D.FUNC	User Function Data may be altered by unauthorized persons

Table 3-2 Threats to TSF Data for the TOE

Threat	Affected asset	Description
T.PROT.ALT	D.PROT	TSF Protected Data may be altered by unauthorized persons
T.CONF.DIS	D.CONF	TSF Confidential Data may be disclosed to unauthorized persons
T.CONF.ALT	D.CONF	TSF Confidential Data may be altered by unauthorized persons

3.3 Organizational Security Policies for the TOE

This section describes the Organizational Security Policies (OSPs) that apply to the TOE. OSPs are used to provide a basis for Security Objectives that are commonly desired by TOE Owners in this operational environment but for which it is not practical to universally define the assets being protected or the threats to those assets.

Table 3-3 Organizational Security Policies for the TOE

Name	Definition
P.USER.AUTHORIZATION	To preserve operational accountability and security, Users will be authorized to use the TOE only as permitted by the TOE Owner.
P.SOFTWARE.VERIFICATION	To detect corruption of the executable code in the TSF, procedures will exist to self-verify executable code in the TSF.
P.AUDIT.LOGGING	To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created, maintained, and protected from unauthorized disclosure or alteration, and will be reviewed by authorized personnel.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its IT environment.
P.HDD.CRYPTO	The Data stored in an HDD must be encrypted to improve the secrecy.

3.4 Assumptions

The Security Objectives and Security Functional Requirements defined in subsequent sections of this Protection Profile are based on the condition that all of the assumptions described in this section are satisfied.

Table 3-4 Assumptions for the TOE

Assumptions	Definition
A.ACCESS.MANAGED	The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.
A.USER.TRAINING	TOE Users are aware of the security policies and procedures of their organization and are trained and competent to follow those policies and procedures.
A.ADMIN.TRAINING	Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.
A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.

4 Security Objectives

4.1 Security Objectives for the TOE

This section describes the Security Objectives that the TOE shall fulfill.

Table 4-1 Security Objectives for the TOE

Objective	Definition
O.DOC.NO_DIS	The TOE shall protect User Document Data from unauthorized disclosure.
O.DOC.NO_ALT	The TOE shall protect User Document Data from unauthorized alteration.
O.FUNC.NO_ALT	The TOE shall protect User Function Data from unauthorized alteration.
O.PROT.NO_ALT	The TOE shall protect TSF Protected Data from unauthorized alteration.
O.CONF.NO_DIS	The TOE shall protect TSF Confidential Data from unauthorized disclosure.
O.CONF.NO_ALT	The TOE shall protect TSF Confidential Data from unauthorized alteration.
O.USER.AUTHORIZED	The TOE shall require identification and authentication of Users and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE.
O.INTERFACE.MANAGED	The TOE shall manage the operation of external interfaces in accordance with security policies.
O.SOFTWARE.VERIFIED	The TOE shall provide procedures to self-verify executable code in the TSF.
O.AUDIT.LOGGED	The TOE shall create and maintain a log of TOE use and security-relevant events and prevent its unauthorized disclosure or alteration.
O.HDD.CRYPTO	The TOE shall encrypt data at the time of storing it to an HDD.

4.2 Security Objectives for the IT environment

This section describes the Security Objectives that must be fulfilled by IT methods in the IT environment of the TOE.

Table 4-2 Security Objectives for the IT environment

Objective	Definition
OE.AUDIT_STORAGE.PROTECTED	If audit records are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records are protected from unauthorized access, deletion and modifications.
OE.AUDIT_ACCESS.AUTHORIZED	If audit records generated by the TOE are exported from the TOE to another trusted IT product, the TOE Owner shall ensure that those records can be accessed in order to detect potential security violations, and only by authorized persons.
OE.INTERFACE.MANAGED	The IT environment shall provide protection from unmanaged access to TOE external interfaces.

4.3 Security Objectives for the non-IT environment

This section describes the Security Objectives that must be fulfilled by non-IT methods in the non-IT environment of the TOE.

Table 4-3 Security Objectives for the non-IT environment

Objective	Definition
OE.PHYSICAL.MANAGED	The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.
OE.USER.AUTHORIZED	The TOE Owner shall grant permission to Users to be authorized to use the TOE according to the security policies and procedures of their organization.
OE.USER.TRAINED	The TOE Owner shall ensure that Users are aware of the security policies and procedures of their organization and have the training and competence to follow those policies and procedures.
OE.ADMIN.TRAINED	The TOE Owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization; have the training, competence, and time to follow the manufacturer's guidance and documentation; and correctly configure and operate the TOE in accordance with those policies and procedures.
OE.ADMIN.TRUSTED	The TOE Owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.
OE.AUDIT.REVIEWED	The TOE Owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

4.4 Security Objectives rationale

This section demonstrates that each threat, organizational security policy, and assumption are mitigated by at least one security objective for the TOE, and that those Security Objectives counter the threats, enforce the policies, and uphold the assumptions.

Table 4-4 Completeness of Security Objectives

Threats, policies, and assumptions	Objectives																		
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.HDD.CRYPTO	OE.AUDIT_STORAGE.PROTECTED	OE.AUDIT_ACCESS.AUTHORIZED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	OE.PHYSICAL.MANAGED	OE.INTERFACE.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED
T.DOC.DIS	X						X	X												
T.DOC.ALT		X					X	X												
T.FUNC.ALT			X				X	X												
T.PROT.ALT				X			X	X												
T.CONF.DIS					X		X	X												
T.CONF.ALT						X	X	X												
P.USER.AUTHORIZATION							X	X												
P.SOFTWARE.VERIFICATION									X											
P.AUDIT.LOGGING										X		X	X	X						
P.INTERFACE.MANAGEMENT															X		X			
P.HDD.CRYPTO											X									
A.ACCESS.MANAGED																X				
A.ADMIN.TRAINING																		X		
A.ADMIN.TRUST																			X	
A.USER.TRAINING																				X

Table 4-5 Sufficiency of Security Objectives

Threats. Policies, and assumptions	Summary	Objectives and rationale
T.DOC.DIS	User Document Data may be disclosed to unauthorized persons.	O.DOC.NO_DIS protects D.DOC from unauthorized disclosure.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.DOC.ALT	User Document Data may be altered by unauthorized persons.	O.DOC.NO_ALT protects D.DOC from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.FUNC.ALT	User Function Data may be altered by unauthorized persons.	O.FUNC.NO_ALT protects D.FUNC from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.PROT.ALT	TSF Protected Data may be altered by unauthorized persons.	O.PROT.NO_ALT protects D.PROT from unauthorized alteration.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization.
T.CONF.DIS	TSF Confidential Data may be disclosed to unauthorized persons.	O.CONF.NO_DIS protects D.CONF from unauthorized disclosure.
		O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
T.CONF.ALT	TSF Confidential Data may be altered by	O.CONF.NO_ALT protects D.CONF from unauthorized alteration.

	unauthorized persons.	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
P.USER.AUTHORIZATION	Users will be authorized to use the TOE	O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization to use the TOE.
		OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization
P.SOFTWARE.VERIFICATION	Procedures will exist to self- verify executable code in the TSF.	O.SOFTWARE.VERIFIED provides procedures to self-verify executable code in the TSF.
P.AUDIT.LOGGING	An audit trail of TOE use and security-relevant events will be created, maintained, protected, and reviewed.	O.AUDIT.LOGGED creates and maintains a log of TOE use and security-relevant events and prevents unauthorized disclosure or alteration.
		OE.AUDIT_STORAGE.PROTECTED protects exported audit records from unauthorized access, deletion, and modifications.
		OE.AUDIT_ACCESS.AUTHORIZED establishes responsibility of, the TOE Owner to provide appropriate access to exported audit records.
		OE.AUDIT.REVIEWED establishes responsibility of the TOE Owner to ensure that audit logs are appropriately reviewed.
P.INTERFACE.MANAGEMENT	Operation of external interfaces will be controlled by the TOE and its IT environment.	O.INTERFACE.MANAGED manages the operation of external interfaces in accordance with security policies.
		OE.INTERFACE.MANAGED establishes a protected environment for TOE external interfaces.
P.HDD.CRYPTO	Cryptographic operation will be controlled by the TOE.	O.HDD.CRYPTO encrypts data stored in HDD by the TOE.
A.ACCESS.MANAGED	The TOE environment provides protection from unmanaged access to the physical components and data interfaces of the TOE.	OE.PHYSICAL.MANAGED establishes a protected physical environment for the TOE.
A.ADMIN.TRAINING	TOE Users are aware of and trained to follow security policies and procedures.	OE.ADMIN.TRAINED establishes responsibility of the TOE Owner to provide appropriate Administrator training.

A.ADMIN.TRUST	Administrators do not use their privileged access rights for malicious purposes.	OE.ADMIN.TRUSTED establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.
A.USER.TRAINING	Administrators are aware of and trained to follow security policies and procedures.	OE.USER.TRAINED establishes responsibility of the TOE Owner to provide appropriate User training.

5 Extended components definition (APE_ECD)

This Protection Profile defines components that are extensions to Common Criteria 3.1 Revision 2, Part 2. These extended components are defined in the Protection Profile but are used in SFR Packages and, therefore, are employed only in TOEs whose STs conform to those SFR Packages.

5.1 FPT_FDI_EXP Restricted forwarding of data to external interfaces

Family behaviour:

This family defines requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Many products receive information on specific external interfaces and are intended to transform and process this information before it is transmitted on another external interface. However, some products may provide the capability for attackers to misuse external interfaces to violate the security of the TOE or devices that are connected to the TOE's external interfaces. Therefore, direct forwarding of unprocessed data between different external interfaces is forbidden unless explicitly allowed by an authorized administrative role. The family FPT_FDI_EXP has been defined to specify this kind of functionality.

Component leveling:

FPT_FDI_EXP.1	Restricted forwarding of data to external interfaces	1

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces provides for the functionality to require TSF controlled processing of data received over defined external interfaces before these data are sent out on another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

The following actions could be considered for the management functions in FMT:

Definition of the role(s) that are allowed to perform the management activities

Management of the conditions under which direct forwarding can be allowed by an administrative role

Revocation of such an allowance

Audit: **FPT_FDI_EXP.1**

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

There are no auditable events foreseen.

Rationale:

Quite often, a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data are allowed to be transferred to another external interface. Examples are firewall systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i.e., without processing the data first) between different external interfaces is therefore a function that—if allowed at all—can only be allowed by an authorized role.

It has been viewed as useful to have this functionality as a single component that allows specifying the property to disallow direct forwarding and require that only an authorized role can allow this. Since this is a function that is quite common for a number of products, it has been viewed as useful to define an extended component.

The Common Criteria defines attribute-based control of user data flow in its FDP class. However, in this Protection Profile, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It was found that using FDP_IFF and FDP_IFC for this purpose resulted in SFRs that were either too implementation-specific for a Protection Profile or too unwieldy for refinement in a Security Target. Therefore, the authors decided to define an extended component to address this functionality.

This extended component protects both user data and TSF data, and it could therefore be placed in either the FDP or FPT class. Since its purpose is to protect the TOE from misuse, the authors believed that it was most appropriate to place it in the FPT class. It did not fit well in any of the existing families in either class, and this lead the authors to define a new family with just one member.

FPT_FDI_EXP.1	**Restricted forwarding of data to external interfaces** **Hierarchical to: No other components** **Dependencies: FMT_SMF.1 Specification of Management Functions** **FMT_SMR.1 Security roles**
FPT_FDI_EXP.1.1	The TSF shall provide the capability to restrict data received on [assignment: *list of external interfaces*] from being forwarded without further processing by the TSF to [assignment: *list of external interfaces*].

6 Security Requirements

In this chapter, the security requirements are described.

6.1 Security functional requirements

In this chapter, the TOE security functional requirements for achieving the security objectives specified in Chapter 4.1 are described. This is quoted from the security functional requirements specified in the CC Part 2. The security functional requirements which are not specified in the CC Part 2 are quoted from the extended security functional requirements specified in the PP (IEEE Std 2600.2-2009).

< Method of specifying security functional requirement "Operation" >

In the following description, when items are **indicated in "bold,"** it means that they are completed or refined. 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.

6.1.1 Class FAU: Security audit

FAU_GEN.1 **Audit data generation**

Hierarchical to : No other components

Dependencies : FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;

- All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and

- **All Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 6-1;** [assignment: *other specifically defined auditable events*]

[selection, choose one of: *minimum, basic, detailed, not specified*]

not specified

[assignment: *other specifically defined auditable events*]

None

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **for each Relevant SFR listed in Table 6-1: (1) the information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required);** [assignment: *other audit relevant information*]

[assignment: *other audit relevant information*]

None

Table 6-1 Audit data requirements

Auditable event	Relevant SFR	Audit level	Additional information	Details
Unsuccessful use of the authentication mechanism	FIA_UAU.1	Minimum	None required	-Failure of login
The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	FIA_AFL.1	Minimum	None required	-Suspension of authentication -Recovery to normal state
Unsuccessful use of the identification mechanism	FIA_UID.1	Minimum	Attempted user identity, if available	-Failure of login
Use of the management functions	FMT_SMF.1	Minimum	None required	Use of the management functions
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None required	No record because no group of users as a role does not exist.
Failure of the trusted channel functions	FTP_ITC.1	Minimum	None required	Failure of the trusted channel functions
Changes to the time	FPT_STM.1	Minimum	None required	changes to the time

FAU_GEN.2 User identity association

Hierarchical to : No other components

Dependencies : FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review

Hierarchical to : No other components

Dependencies : FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.

[assignment: *authorised users*]

U.ADMINISTRATOR

[assignment: *list of audit information*]

Audit log indicated in Table 6-1

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

Hierarchical to : No other components

Dependencies : FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_STG.1 Protected audit trail storage

Hierarchical to : No other components

Dependencies : FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [selection, choose one of*: prevent, detect*] unauthorised modifications to the stored audit records in the audit trail.

[selection, choose one of*: prevent, detect*]

prevent

FAU_STG.4(1) Prevention of audit data loss

Hierarchical to : FAU_STG.3 Action in case of possible audit data loss

Dependencies : FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full ***(if the audit trail is full, in the state where operation when the audit trail was full was set as "overwrite prohibition")***.

[selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]

ignore audited events

[assignment: *other actions to be taken in case of audit storage failure*]
Suspend acceptance of jobs

FAU_STG.4(2) Prevention of audit data loss

Hierarchical to : FAU_STG.3 Action in case of possible audit data loss
Dependencies : FAU_GEN.1 Audit data generation

FAU_STG.4.1 The TSF shall [selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full ***(if the audit trail is full, in the state where operation when the audit trail was full was set as "overwrite permission").***
[selection, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]
overwrite the oldest stored audit records
[assignment: *other actions to be taken in case of audit storage failure*]
None

6.1.2 Class FCS: Cryptographic support

FCS_CKM.1 Cryptographic key generation

Hierarchical to : No other components.
Dependencies : [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys ***(cryptographic keys for HDD encryption)*** in accordance with a specified cryptographic key generation algorithm [assignment: cryptographic key generation algorithm] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].
[assignment: cryptographic key generation algorithm]
refer to Table 6-2
[assignment: cryptographic key sizes]
refer to Table 6-2
[assignment: list of standards]
refer to Table 6-2

Table 6-2 Cryptographic key algorithm key size

list of standards	cryptographic key generation algorithm	key sizes
Konica Minolta Encryption specification standard	Konica Minolta HDD Encryption Key Generation Algorithm	-256 bit

FCS_COP.1 Cryptographic operation

Hierarchical to : No other components

Dependencies : [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

..FCS_COP.1.1 The TSF shall perform [assignment: list of cryptographic operations] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

[assignment: list of cryptographic operations]
refer to Table 6-3
[assignment: cryptographic algorithm]
refer to Table 6-3
[assignment: cryptographic key sizes]
refer to Table 6-3
[assignment: list of standards]
refer to Table 6-3

Table 6-3 Cryptographic operations algorithm key size standards

Standard	cryptographic algorithm	key sizes	cryptographic operations
FIPS PUB197	AES	-256 bit	Encrypt HDD

6.1.3 Class FDP: User data protection

FDP_ACC.1(a) Subset access control

Hierarchical to : No other components

Dependencies : FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(a) The TSF shall enforce the Common Access Control SFP in Table 17 (*Access Control SFP in Table 6-4,Table 6-5,Table 6-6,Table 6-7,Table 6-8,Table 6-9)* on the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in Table 17 (*the list of users as subjects, objects, and operations among subjects and objects covered by the Access Control SFP in Table 6-4,Table 6-5,Table 6-6,Table 6-7,Table 6-8,Table 6-9)*.

Table 6-4 Common Access Control SFP

Object	Attribute		Operation(s)	Subject	Subject Attribute	Access control rule
	Function Attribute	Object Attribute				
D.DOC	+SCN +CPY +FAXOUT	User ID	Delete	U.NORMAL	User ID	Operation is permitted, only when User ID matches.
D.FUNC	+PRT	Box Type User ID	Modify Delete	U.NORMAL	User ID	Operation is permitted, only to the one whose user ID matches, when Box Type is not Secure print user box.
		Box Type DOC PASSWORD	Modify Delete	U.NORMAL	DOC PASSWORD	Operation is permitted, only when DOC PASSWORD matches, when Box Type is Secure print user box.
	+CPY +SCN +FAXOUT	User ID	Modify Delete	U.NORMAL	User ID	Operation is permitted, only when User ID matches.
	+DSR +FAXIN	Box Type sBOX PASSWORD	Delete	U.NORMAL	sBOX PASSWORD	Operation is permitted, only when sBOX PASSWORD matches, when Box Type is Memory RX user box.
	+DSR	Box Type sBOX PASSWORD	Modify Delete	U.NORMAL	sBOX PASSWORD	Operation is permitted, only when sBOX PASSWORD matches, when Box Type is Annotation user box.

Table 6-5 PRT Access Control SFP

Object	Attribute		Operation(s)	Subject	Subject Attribute	Access control rule
	Function Attribute	Object Attribute				
D.DOC	+PRT	Box Type User ID	Read Delete	U.NORMAL	User ID	Operation is permitted only to the one whose user ID matches, when Box Type is not Secure Print user box.
		Box Type DOC PASSWORD	Read Delete	U.NORMAL	DOC PASSWORD	Operation is permitted, only when DOC PASSWORD matches, when Box Type is Secure print user box.

※It is specified by referring to BOX TYPE, since DOC PASSWORD is added corresponding to BOX TYPE.

Table 6-6 SCN Access Control SFP

Object	Attribute		Operation(s)	Subject	Subject Attribute	Access control rule
	Function Attribute	Object Attribute				
D.DOC	+SCN	User ID	Read Modify	U.NORMAL	User ID	Operation is permitted only to the one whose user ID matches.

Table 6-7 CPY Access Control SFP

Object	Attribute		Operation(s)	Subject	Subject Attribute	Access control rule
	Function Attribute	Object Attribute				
D.DOC	+CPY	User ID	Read	U.NORMAL	User ID	Operation is permitted only to the one whose user ID matches.

Table 6-8 FAX Access Control SFP

Object	Attribute		Operation(s)	Subject	Subject Attribute	Access control rule
	Function Attribute	Object Attribute				
D.DOC	+ FAXIN	Box Type sBox PASSWORD	Delete Read	U.NORMAL	sBOX PASSWORD	Operation is permitted, only when sBOX PASSWORD matches, when Box Type is Memory RX user box.
	+FAXOUT	User ID	Read Modify	U.NORMAL	User ID	Operation is permitted only to the one whose user ID matches.

Table 6-9 DSR Access Control SFP

Object	Attribute		Operation(s)	Subject	Subject Attribute	Access control rule
	Function Attribute	Object Attribute				
D.DOC	+DSR	Box Type sBOX PASSWORD	Delete Read	U.NORMAL	sBOX PASSWORD	Operation is permitted, only when sBOX PASSWORD matches, when Box Type is annotation user box.
						Operation is permitted, only when sBOX PASSWORD matches, when Box Type is Memory RX user box.

FDP_ACC.1(b) Subset access control

Hierarchical to : No other components

Dependencies : FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP** (***TOE Function Access Control SFP in Table 6-10)*** on **users as subjects, TOE functions as objects, and the right to use the functions as operations** (***the list of users as subjects, objects, and operations among subjects and objects covered by the TOE Function Access Control***

SFP in Table 6-10).

Table 6-10 TOE Function Access Control SFP

Object (TOE Function)	Object Attribute	Operation(s)	Subject	Subject Attribute	Access control rule
F.PRT	Permission Role	Execution	U.NORMAL	Allocation Role	Execution of the function is permitted, when Allocation Role that is a Subject includes Permission Role that is an Object.
F.SCN	Permission Role	Execution	U.NORMAL	Allocation Role	Execution of the function is permitted, when Allocation Role that is a Subject includes Permission Role that is an Object.
F.CPY	Permission Role	Execution	U.NORMAL	Allocation Role	Execution of the function is permitted, when Allocation Role that is a Subject includes Permission Role that is an Object.
F.FAX	Permission Role	Execution	U.NORMAL	Allocation Role	Execution of the function is permitted, when Allocation Role that is a Subject includes Permission Role that is an Object.
F.DSR	Permission Role	Execution	U.NORMAL	Allocation Role	Execution of the function is permitted, when Allocation Role that is a Subject includes Permission Role that is an Object.

FDP_ACF.1(a) Security attribute based access control

: Hierarchical to : No other components
Dependencies : FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(a) The TSF shall enforce the **Common Access Control SFP in Table 17** (*Access Control SFP in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, Table 6-9)* to objects based

on the following: the list of users as subjects and objects controlled under the Common Access Control SFP in Table 17, and for each, the indicated security attributes in Table 17 (*the list of users as subjects and objects controlled under the Access Control SFP in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, Table 6-9 and for each, the indicated security attributes in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, Table 6-9)*.

FDP_ACF.1.2(a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: rules specified in the Common Access Control SFP in Table 17 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects (*rules specified in the Document Access Control SFP in Table 6-4,Table 6-5,Table 6-6,Table 6-7,Table 6-8,Table 6-9 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects)*.

FDP_ACF.1.3(a) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].
[assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
- U.ADMINISTRATOR can delete all D.DOC and D.FUNC.
- Anybody can Delete by cancelling FAX communication during receiving all D_DOC and D_FUNC which have +FAXIN attribute.

FDP_ACF.1.4(a) 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*].
- The access to the user box is prohibited when number of continuous mismatch of sBOX PASSWORD reached the administrator configurable positive integer within 1-3.
- The access to the secure print is prohibited when number of continuous mismatch of DOC PASSWORD reached the administrator configurable positive integer within 1-3.

FDP_ACF.1(b) Security attribute based access control

Hierarchical to : No other components
Dependencies : FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(b) The TSF shall enforce the TOE Function Access Control SFP (*TOE Function Access Control SFP in Table 6-10)* to objects based on the following: **users and [assignment: *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP*]**.
[assignment: list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP]
the list of users as subjects and objects controlled under the TOE Function Access Control SFP in Table 6-10, and for each, the indicated security attributes in Table 6-10

FDP_ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among

controlled subjects and controlled objects is allowed: **[selection: *the user is explicitly authorized by U.ADMINISTRATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions* [assignment: *list of functions*], [assignment: *other conditions*]]**.
[selection: *the user is explicitly authorized by U.ADMINISTRATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions* [assignment: *list of functions*], [assignment: *other conditions*]]
[assignment: other conditions]
Table 6-10

FDP_ACF.1.3(b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **the user acts *(receives a fax document)* in the role U.ADMINISTRATOR**: [assignment: ***other*** *rules, based on security attributes, that explicitly authorise access of subjects to objects*].
[assignment: ***other*** *rules, based on security attributes, that explicitly authorise access of subjects to objects*].
None

FDP_ACF.1.4(b) 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*].
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*].
None

FDP_RIP.1 Subset residual information protection

Hierarchical to : No other components
Dependencies : No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: **D.DOC**, [assignment: *list of objects*].
[selection: *allocation of the resource to, deallocation of the resource from*]
deallocation of the resource from
[assignment: *list of objects*].
None

6.1.4 Class FIA: Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to : No other components
Dependencies : FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].
[selection: *[assignment: positive integer number], an administrator configurable*

positive integer within[assignment: range of acceptable values]]
an administrator configurable positive integer within[assignment: range of acceptable values]
[assignment: range of acceptable values]
1～3
[assignment: *list of authentication events*]
Authentication of login password

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].
[selection: *met, surpassed*]
met, surpassed
[assignment: *list of actions*]
Suspend authentication by login password
＜Operation for recovering the normal condition＞
Authentication of U.BUILTIN_ADMINISTRATOR: Perform the boot process of the TOE. (Release process is performed after time set in the release time setting of operation prohibition for Administrator authentication passed by the boot process.)
Other (include U.USER_ADMINISTRATOR): Execute the delete function of authentication failure frequency by U.ADMINISTRATOR, who is not in the authentication stopped state.

FIA_ATD.1 User attribute definition

Hierarchical to : No other components
Dependencies : No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].
[assignment: *list of security attributes*].
User ID
Allocation Role
Role

FIA_SOS.1(1) Verification of secrets

Hierarchical to : No other components
Dependencies : No dependencies

FIA_SOS.1.1(1) The TSF shall provide a mechanism to verify that secrets ***(Login password, Secure print password)*** meet [assignment: *a defined quality metric*].
[assignment: *a defined quality metric*]
-Number of characters : 8 or more characters
-Character type : possible to choose from 94 or more characters
-Rule : (1) Do not compose by only one and the same character.
(2) Do not set the same password as the current setting after change.

FIA_SOS.1(2) Verification of secrets

Hierarchical to : No other components

Dependencies : No dependencies

FIA_SOS.1.1(2) The TSF shall provide a mechanism to verify that secrets ***(Encryption passphrase)*** meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]

-Number of characters : 20 characters

-Character type : possible to choose from 83 or more characters

-Rule : (1)Do not compose by only one and the same character

(2)Do not the same password as the current setting after change

FIA_UAU.1 Timing of authentication

Hierarchical to : No other components

Dependencies : FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***] on behalf of the user to be performed before the user is authenticated.

[assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***]

Confirm the suspended state of user's use in MFP authentication

Receive Fax

Set the TOE status confirmation and display, etc.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.7 Protected authentication feedback

Hierarchical to : No other components

Dependencies : FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.

[assignment: *list of feedback*]

Display "*" every character data input.

FIA_UID.1 Timing of identification

Hierarchical to : No other components

Dependencies : No dependencies

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled Functions of the TOE***] on behalf of the user to be performed before the user is identified.

[assignment: *list of TSF-mediated actions* ***that do not conflict with access-controlled***

Functions of the TOE]
Confirm the suspended state of user's use in MFP authentication
Receive RX
Set the TOE status confirmation and display, etc.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject binding

Hierarchical to : No other components
Dependencies : FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].
[assignment: *list of user security attributes*].
User ID
Allocation Role
Role

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with the subjects acting on behalf of users: [assignment: *rules for the initial association of attributes*].
[assignment: *rules for the initial association of attributes*]
None

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes with the subjects acting on behalf of users: [assignment: *rules for the changing of attributes*].
[assignment: *rules for the changing of attributes*]
None

6.1.5 Class FMT: Security management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to : No other components
Dependencies : FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].
[selection: determine the behaviour of, disable, enable, modify the behaviour of]
modify the behaviour of
[assignment: list of functions]
- Enhanced Security Setting
- User Authentication function
- HDD data overwrite deletion function
- Audit Log function
- Trusted Channel function

[assignment: the authorised identified roles].
U.ADMINISTRATOR

FMT_MSA.1(a) Management of security attributes

Hierarchical to : No other components

Dependencies : [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(a) The TSF shall enforce the **Common Access Control SFP in Table 17** ***(Access Control SFP in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, and Table 6-9)***,[assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].
[assignment: *access control SFP(s), information flow control SFP(s)*]
None
[selection: *change_default, query, modify, delete, [assignment: other operations]*]
Refer to Table 6-11, Table 6-12
[assignment: *list of security attributes*]
Refer to Table 6-11, Table 6-12
[assignment: *the authorized identified roles*]
Refer to Table 6-11, Table 6-12

Table 6-11 Management of Object Security Attribute

Access Control SFP	Object Security Attribute	Authorized Identified Roles	Operations
Common Access Control SFP PRT Access Control SFP SCN Access Control SFP CPY Access Control SFP FAX Access Control SFP	User ID	Nobody	Any operation
FAX Access Control SFP	Box Type sBOX PASSWORD	-U.ADMINISTRATOR	Modify and Delete sBOX PASSWORD, when Box Type is Memory RX user box.
	Box Type sBOX PASSWORD	U.ADMINISTRATOR	Modify and Delete
PRT Access Control SFP	DOC PASSWORD	Nobody	Any operation

DSR Access Control SFP	Box Type sBOX PASSWORD	-U.ADMINISTRATOR	Modify and Delete sBOX PASSWORD, when Box Type is Annotation user box.
	Box Type sBOX PASSWORD	U.ADMINISTRATOR	Modify and Delete sBOX PASSWORD, when Box Type is Memory RX user box.

Table 6-12 Management of Subject Security Attribute

Access Control SFP	Subject Security Attribute	Authorized Identified Roles	Operations
Common Access Control SFP PRT Access Control SFP SCN Access Control SFP CPY Access Control SFP FAX Access Control SFP DSR Access Control SFP	User ID	U.ADMINISTRATOR	Create Delete Modify Suspend temporarily Release
PRT Access Control SFP	DOC PASSWORD	Nobody	Any operation
FAX Access Control SFP DSR Access Control SFP	sBOX PASSWORD	Nobody	Any operation

* U.Administrator sets sBOX PASSWORD. Operator inputs (sets) DOC PASSWORD.

FMT_MSA.1(b) Management of security attributes

Hierarchical to : No other components

Dependencies : [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(b) The TSF shall enforce the **TOE Function Access Control SFP**, [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

[assignment: *access control SFP(s), information flow control SFP(s)*]

None

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

Refer to Table 6-13, Table 6-14
[assignment: *list of security attributes*]
Refer to Table 6-13, Table 6-14
[assignment: *the authorised identified roles*]
Refer to Table 6-13, Table 6-14

Table 6-13 Management of Subject Attribute

Access Control SFP	Subject Security Attribute	Authorized Identified Roles	Operations
TOE Function Access Control SFP	Allocation Role	U.ADMINISTRATOR	Delete Modify

Table 6-14 Management of Object Attribute

Access Control SFP	Object Security Attribute	Authorized Identified Roles	Operations
TOE Function Access Control SFP	Permission Role	Nobody	Any operation

FMT_MSA.3(a) Static attribute initialisation

Hierarchical t : No other components
Dependencies: : FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(a) The TSF shall enforce the **Common Access Control SFP in Table 17** (***Access Control SFP in Table 6-4, Table 6-5, Table 6-6, Table 6-7, Table 6-8, Table 6-9)***, [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.
[assignment: *access control SFP, information flow control SFP*]
None
[selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.
[assignment: other property]
refer to Table 6-15

FMT_MSA.3.2(a) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.
[assignment: *the authorized identified roles*]
nobody

Table 6-15 Characteristics Static Attribute Initialization

Access Control SFP	Object	Function Attribute	Object Attribute		Default values for Object Security Attribute
Common Access Control SFP	D.DOC	+SCN +CPY +FAXOUT	User ID		User ID of U.NORMAL who created the left Object
	D.FUNC	+PRT +CPY +SCN +FAXOUT	User ID		User ID of U.NORMAL who created the left Object
		+DSR +FAXIN	Box Type	sBOX PASSWORD	Box Type and sBOX PASSWORD of the user box, when the object is saved in the Annotation user box or Memory RX user box.
PRT Access Control SFP	D.DOC D.FUNC	+PRT	Box Type	User ID	Box Type is Password Encrypted PDF user box, if it's the object of password encrypted PDF. If it's the object of ID & Print, Box Type is ID & Print user box. User ID is the User ID of U.NORMAL who executed printing
				DOC PASSWORD	Box Type is Secure Print user box, when the object is secure print. DOC PASSWORD is the password that is input at the time of generating the object.
SCN Access Control SFP	D.DOC	+SCN	User ID		User ID of U.NORMAL who created the left Object
CPY Access Control SFP	D.DOC	+CPY	User ID		User ID of U.NORMAL who created the left Object
FAX Access Control SFP	D.DOC	+FAXOUT	User ID		User ID of U.NORMAL who created the left Object
		+FAXIN	Box Type	sBOX PASSWORD	Box Type and sBOX PASSWORD of the user box (Memory RX user box), that is the storage of the object.
DSR Access Control	D.DOC	+DSR	Box Type	sBOX PASSWORD	Box Type and sBOX PASSWORD of the user box (Annotation user box), that is the storage of the

SFP					object.

* Multiple Function Attributes are not given at the same time since it is given corresponding to the functions (print, scan, etc.) that generate objects.

FMT_MSA.3(b) Static attribute initialisation

Hierarchical to : No other components
Dependencies: : FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(b) The TSF shall enforce the **TOE Function Access Control Policy** ***(TOE Function Access Control SFP)***, [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.
[assignment: *access control SFP, information flow control SFP*]
None
[selection, choose one of: *restrictive, permissive, [assignment: other property]*]
[assignment: other property]
Refer to Table 6-16

FMT_MSA.3.2(b) The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.
[assignment: *the authorized identified roles*]
nobody

Table 6-16 Characteristics Static Attribute Initialization

Object (TOE Function)	Object Attribute	Characteristics which restricts access only to Subject which any of the following attributes
F.PRT	Permission Role	Print Role
F.SCN	Permission Role	Scan Role
F.CPY	Permission Role	Copy Role
F.FAX	Permission Role	Fax Role
F.DSR	Permission Role	DSR Role

FMT_MTD.1 Management of TSF data

Hierarchical to : No other components
Dependencies: : FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1(a) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to **[selection, choose one of: *Nobody*, [selection: *U.ADMINISTRATOR*,** [assignment: *the authorized identified roles* ***except U.NORMAL***]]].

[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
refer to Table 6-17
[assignment: other operations]
refer to Table 6-17
[assignment: *list of TSF data*]
refer to Table 6-17
[selection, choose one of: *Nobody*, **[selection:** ***U.ADMINISTRATOR,*** [assignment: *the authorized identified roles* ***except U.NORMAL***]]]
refer to Table 6-17

FMT_MTD.1.1(b) The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data* ***associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL***] to **[selection, choose one of:** ***Nobody,*** **[selection:** ***U.ADMINISTRATOR, the U.NORMAL to whom such TSF data are associated***]].
[selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
refer to Table 6-18
[assignment: *list of TSF data* ***associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL***]
refer to Table 6-18
selection, choose one of: ***Nobody,*** **[selection:** ***U.ADMINISTRATOR, the U.NORMAL to whom such TSF data are associated***]]
refer to Table 6-18

Table 6-17 Operation of TSF Data

TSF Data	Authorized Identification Roles	Operations
Login password of U.BUILTIN_ADMINISTRATOR	U.BUILTIN_ADMINISTRATOR	Modify
Encryption Passphrase	U.ADMINISTRATOR	Set Modify
Time Information	U.ADMINISTRATOR	Modify
Auto Reset Time	U.ADMINISTRATOR	Modify
Auto logout time	U.ADMINISTRATOR	Modify
Authentication Failure Frequency Threshold	U.ADMINISTRATOR	Modify
Number of Authentication Failure (except U.BUILTIN_ADMINISTRATOR)	U.ADMINISTRATOR	Clear
Password mismatch frequency threshold	U.ADMINISTRATOR	Modify
Number of Password mismatch	U.ADMINISTRATOR	Clear
Password rule	U.ADMINISTRATOR	Modify
External server authentication setting data	U.ADMINISTRATOR	Register Modify
Release time of operation prohibition for Administrator authentication	U.ADMINISTRATOR	Modify
Network Settings	U.ADMINISTRATOR	Register

		Modify
Transmission address setting	U.ADMINISTRATOR	Register Modify

Table 6-18 Operation of TSF Data

TSF Data	Authorized Identification Roles	Operations
Login Password of U.NORMAL	U.ADMINISTRATOR	Register
	U.ADMINISTRATOR	Modify
	User who is related with the password (U.NORMAL)	
Role	U.ADMINISTRATOR	Addition and Deletion of U.USER_ADMINISTRATOR

FMT_SMF.1 Specification of Management Functions

Hierarchical to : No other components

Dependencies: : No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].

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

refer to Table 6-19

Table 6-19 list of management functions

management functions
Management function of Enhanced Security Setting by U.ADMINISTRATOR
Management function of User Authentication function by U.ADMINISTRATOR
Operation setting function of HDD data overwrite deletion function by U.ADMINISTRATOR
Audit log management function by U.ADMINISTRATOR
Trusted Channel management function by U.ADMINISTRATOR
User management function by U.ADMINISTRATOR
Temporary suspension and Release function of User ID of U.NORMAL by U.ADMINISTRATOR
Registration and modification function of U.NORMAL's login password by U.ADMINISTRATOR
Modification function of one's own login password by U.NORMAL
Modification function of one's own login password by U.BUILTIN_ADMINISTRATOR
Setting and modification function of encryption passphrase by U.ADMINISTRATOR
Modification function of date and time information by U.ADMINISTRATOR
Modification function of auto reset time by U.ADMINISTRATOR
Modification function of auto logout time by U.ADMINISTRATOR
Modification function of Authentication failure frequency threshold by U.ADMINISTRATOR
Registration and modification function of External server authentication setting data by U.ADMINISTRATOR
Modification function of release time of operation prohibition of administrator authentication by

U.ADMINISTRATOR Deletion function of Password mismatch frequency by U.ADMINISTRATOR Modification function of Password mismatch frequency threshold by U.ADMINISTRATOR Deletion function of Authentication failure frequency (except administrator) by U.ADMINISTRATOR Modification function of Password policy by U.ADMINISTRATOR Registration and Modification function of Network setting by U.ADMINISTRATOR Registration and Modification function of transmission address by U.ADMINISTRATOR Management function of Object security attributes (except User ID, Box Type, DOC PASSWORD) by U.ADMINISTRATOR Management function of Subject security attributes (except object of management by user management function, Temporary suspension and release of User ID, sBOX PASSWORD, DOC PASSWORD) by U.ADMINISTRATOR Management function of Role (except Role of U.BUILTIN_ADMINISTRATOR) by U.ADMINISTRATOR

FMT_SMR.1 Security roles

Hierarchical to : No other components

Dependencies: : FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles **U.ADMINISTRATOR, U.NORMAL, [selection: *Nobody*,** [assignment: *the authorised identified roles*]].

[selection: *Nobody*, [assignment: *the authorised identified roles*]]

Nobody

FMT_SMR.1.2 The TSF shall be able to associate users with roles, **except for the role "Nobody" to which no user shall be associated**.

6.1.6 Class FPT: Protection of the TSF

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to : No other components

Dependencies: : FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on **any external Interface** from being forwarded without further processing by the TSF to **any Shared-medium Interface**.

FPT_STM.1 Reliable time stamps

Hierarchical to : No other components

Dependencies: : No dependencies

FPT_STM.1.1 TSF shall be able to provide reliable time stamps.

FPT_TST.1 TSF testing

Hierarchical to : No other components

Dependencies: : No dependencies

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].

[selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occur*]]

during initial start-up

[selection: [assignment: *parts of TSF*], *the TSF*]

[assignment: parts of TSF]

HDD Encryption Function

TSF executable code

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF*], *TSF data*].

[selection: [assignment: *parts of TSF*], *TSF data*].

[assignment: parts of TSF]

Encryption passphrase

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

6.1.7 Class FTA: TOE access

FTA_SSL.3 TSF-initiated termination

Hierarchical to : No other components

Dependencies: : No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

[assignment: *time interval of user inactivity*]

- Time decided by the auto reset time in case of operation panel.

- Time decided by auto logout time in case of Web Connection

- 60 minutes in case of Data Administrator

- No interactive session in case of printer driver or fax.

6.1.8 Class FTP: Trusted path/channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to : No other components

Dependencies: : No dependencies

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from

modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **the TSF, another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **communication of D.DOC, D.FUNC, D.PROT, and D.CONF over any Shared-medium Interface**.

6.2 Security assurance requirements

Table 6-20 lists the security assurance requirements for 2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B, and related SFR packages, EAL 2 augmented by ALC_FLR.2.

Table 6-20 IEEE 2600.2 Security Assurance Requirements

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures (augmentation of EAL2)
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing—sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.3 Security requirements rationale

6.3.1 Common security requirements rationale

Table 6-21 and Table 6-22 demonstrate the completeness and sufficiency of SFRs that fulfill the objectives of the TOE. **Bold typeface** items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

Table 6-21 Completeness of security requirements

SFRs	Objectives										
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.HDD.CRYPTO
FAU_GEN.1										**P**	
FAU_GEN.2										**P**	
FAU_SAR.1										**P**	
FAU_SAR.2										**P**	
FAU_STG.1										**P**	
FAU_STG.4(1)										**P**	
FAU_STG.4(2)										**P**	
FCS_CKM.1											**P**
FCS_COP.1											**P**
FDP_ACC.1(a)	**P**	**P**	**P**								
FDP_ACC.1(b)							**P**				
FDP_ACF.1(a)	S	S	S								
FDP_ACF.1(b)							S				
FDP_RIP.1	**P**										
FIA_AFL.1							S	S			
FIA_ATD.1							S				
FIA_SOS.1(1)	S	S	S				S	S			
FIA_SOS.1(2)											S
FIA_UAU.1							**P**	**P**			
FIA_UAU.7							S	S			
FIA_UID.1	S	S	S	S	S	S	**P**	**P**		S	S
FIA_USB.1							**P**				
FMT_MOF.1	S	S	S	S	S	S	S	S		S	S
FMT_MSA.1(a)	S	S	S	**P**	**P**	**P**					
FMT_MSA.1(b)				**P**			S				
FMT_MSA.3(a)	S	S	S								
FMT_MSA.3(b)							S				
FMT_MTD.1				**P**	**P**	**P**					S
FMT_SMF.1	S	S	S	S	S	S	S	S		S	S
FMT_SMR.1	S	S	S	S	S	S	S				S
FPT_FDI_EXP.1								**P**			

SFRs	Objectives										
	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	O.HDD.CRYPTO
FPT_STM.1										S	
FPT_TST.1									**P**		
FTA_SSL.3							**P**	**P**			
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**					

Table 6-22 Sufficiency of security requirements

Objectives	Description	SFRs	Purpose
O.DOC.NO_DIS, O.DOC.NO_ALT, O.FUNC.NO_ALT	Protection of User Data from unauthorized disclosure or alteration	**FDP_ACC.1(a)**	**Enforces protection by establishing an access control policy.**
		FDP_ACF.1(a)	Supports access control policy by providing access control function.
		FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MOF.1	Supports protection by management of security functions behavior.
		FMT_MSA.1(a)	Supports access control function by enforcing control of security attributes.
		FMT_MSA.3(a)	Supports access control function by enforcing control of security attribute defaults.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.
		FTP_ITC.1	**Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.**
		FIA_SOS.1(1)	Supports authorization by requiring by specification of secrets.
O.DOC.NO_DIS	Protection of User	**FDP_RIP.1**	**Enforces protection by making**

	Document Data from unauthorized disclosure		**residual data unavailable.**
O.PROT.NO_ALT,	Protection of TSF Data from unauthorized alteration	FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MOF.1	Supports protection by management of security functions behavior.
		FMT_MSA.1(a)	**Supports access control function by enforcing control of security attributes.**
		FMT_MSA.1(b)	**Supports access control function by enforcing control of security attributes.**
		FMT_MTD.1	**Enforces protection by restricting access.**
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.
		FTP_ITC.1	**Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.**
O.CONF.NO_DIS, O.CONF.NO_ALT	Protection of TSF Data from unauthorized disclosure or alteration	FIA_UID.1	Supports access control and security roles by requiring user identification.
		FMT_MOF.1	Supports protection by management of security functions behavior.
		FMT_MSA.1(a)	**Supports access control function by enforcing control of security attributes.**
		FMT_MTD.1	**Enforces protection by restricting access.**
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports control of security attributes by requiring security roles.

		FTP_ITC.1	**Enforces protection by requiring the use of trusted channels for communication of data over Shared-medium Interfaces.**
O.USER_AUTHORIZED	Authorization of Normal Users and Administrators to use the TOE	**FDP_ACC.1(b)**	**Enforces authorization by establishing an access control policy.**
		FDP_ACF.1(b)	Supports access control policy by providing access control function.
		FIA_AFL.1	Enforces authorization by requiring access control.
		FIA_ATD.1	Supports authorization by associating security attributes with users.
		FIA_SOS.1(1)	Supports authorization by requiring by specification of secrets.
		FIA_UAU.1	**Enforces authorization by requiring user authentication.**
		FIA_UAU.7	Enforces authorization by requiring user authentication.
		FIA_UID.1	**Enforces authorization by requiring user identification.**
		FIA_USB.1	**Enforces authorization by distinguishing subject security attributes associated with user roles.**
		FMT_MOF.1	Supports protection by management of security functions behavior.
		FMT_MSA.1(b)	Supports access control function by enforcing control of security attributes.
		FMT_MSA.3(b)	Supports access control function by enforcing control of security attribute defaults.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR 1	Supports authorization by requiring security roles.
		FTA_SSL.3	**Enforces authorization by terminating inactive sessions.**
O.INTERFACE.MANAGED	Management of external interfaces	**FIA_AFL.1**	Enforces authorization by requiring access control.
		FIA_SOS.1(1)	Supports authorization by requiring by specification of secrets.

		FIA_UAU.1	**Enforces management of external interfaces by requiring user authentication.**
		FIA_UAU.7	Enforces authorization by requiring user authentication.
		FIA_UID.1	**Enforces management of external interfaces by requiring user authentication.**
		FMT_MOF.1	Supports protection by management of security functions behavior.
		FMT_SMF 1	Supports control of security attributes by requiring functions to control attributes.
		FPT_FDI_EXP.1	**Enforces management of external interfaces by requiring (as needed) administrator control of data transmission from external Interfaces to Shared-medium Interfaces.**
		FTA_SSL.3	**Enforces management of external interfaces by terminating inactive sessions.**
O.SOFTWARE.VERIFIED	Verification of software integrity	**FPT_TST.1**	**Enforces verification of software by requiring self-tests.**
O.AUDIT.LOGGED	Logging and authorized access to audit events	**FAU_GEN.1**	**Enforces audit policies by requiring logging of relevant events.**
		FAU_GEN.2	**Enforces audit policies by requiring logging of information associated with audited events.**
		FAU_SAR.1	**Enforces audit policies by providing security audit record.**
		FAU_SAR.2	**Enforces audit policies by restricting reading of security audit records.**
		FAU_STG.1	**Enforces audit policies by protecting from unauthorised deletion and/or modification.**
		FAU_STG.4(1)	**Enforces audit policies by preventing audit data loss.**
		FAU_STG.4(2)	**Enforces audit policies by preventing audit data loss.**
		FIA_UID.1	Enforces management of external interfaces by requiring user authentication.
		FMT_MOF.1	Supports protection by management of security functions behavior.

		FMT_SMF 1	Supports control of security attributes by requiring functions to control attributes.
		FPT_STM.1	Supports audit policies by requiring time stamps associated with events.
O.HDD.CRYPTO	The encryption of data	FCS_CKM.1	Generates encryption key
		FCS_COP.1	Encrypts
		FIA_SOS.1(2)	Verifies the quality of the data which is the source of the encryption key
		FIA_UID.1	Enforces authorization by requiring user identification.
		FMT_MOF.1	Supports protection by management of security functions behavior.
		FMT_MTD.1	Enforces protection by restricting access.
		FMT_SMF.1	Supports control of security attributes by requiring functions to control attributes.
		FMT_SMR.1	Supports authorization by requiring security roles.

6.3.1.1 The dependencies of security requirements

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

Table 6-23 The dependencies of security requirements

Functional Requirements Component for this ST	Dependencies on CC Part2	Dependencies Relation in this ST
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4(1)	FAU_STG.1	FAU_STG.1
FAU_STG.4(2)	FAU_STG.1	FAU_STG.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1 <The rationale not to apply FCS_CKM.4> The encryption key is used for encrypting HDD data and generated when turning the power ON. The generated key is stored in the volatile memory, but there is no necessity to consider the encryption key destruction since no external interface to access this key is not provided and the physical access to the

Functional Requirements Component for this ST	Dependencies on CC Part2	Dependencies Relation in this ST
		memory is limited in the operational environment.
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 <The rationale not to apply FCS_CKM.4> The encryption key is used for encrypting HDD data and generated when turning the power ON. The generated key is stored in the volatile memory, but there is no necessity to consider the encryption key destruction since no external interface to access this key is not provided and the physical access to the memory is limited in the operational environment.
FDP_ACC.1(a)	FDP_ACF.1	FDP_ACF.1(a)
FDP_ACC.1(b)	FDP_ACF.1	FDP_ACF.1(b)
FDP_ACF.1(a)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(a) FMT_MSA.3(a)
FDP_ACF.1(b)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(b) FMT_MSA.3(b)
FDP_RIP.1	None	N/A
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	None	N/A
FIA_SOS.1(1)	None	N/A
FIA_SOS.1(2)	None	N/A
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	None	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1(a)	[FDP_ACC.1 orFDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(a) FMT_SMR.1 FMT_SMF.1
FMT_MSA.1(b)	[FDP_ACC.1 orFDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(b) FMT_SMR.1 FMT_SMF.1
FMT_MSA.3(a)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(a) FMT_SMR.1
FMT_MSA.3(b)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(b) FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_STM.1	None	N/A
FPT_TST.1	None	N/A
FTA_SSL.3	None	N/A
FTP_ITC.1	None	N/A
FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1

6.3.2 Security assurance requirements rationale

This Protection Profile has been developed for Hardcopy Devices to be used in commercial information processing environments that require a moderate level of document security, network security, and security assurance. The TOE will be exposed to only a low level of risk because it is assumed that the TOE will be located in a restricted or monitored environment that provides almost constant protection from unauthorized and unmanaged access to the TOE and its data interfaces. Agents cannot physically access any nonvolatile storage without disassembling the TOE except for removable nonvolatile storage devices, where protection of User and TSF Data are provided when such devices are removed from the TOE environment. Agents have limited or no means of infiltrating the TOE with code to effect a change, and the TOE self-verifies its executable code to detect unintentional malfunctions. As such, the Evaluation Assurance Level 2 is appropriate.
EAL 2 is augmented with ALC_FLR.2, Flaw reporting procedures. ALC_FLR.2 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place, and their inclusion is expected by the consumers of this TOE.

7 TOE Summary specification

The list of the TOE security functions led from the TOE security functional requirements is shown in Table 7-1. The detail is explained in the paragraph described below.

Table 7-1 Names and identifiers of TOE Security Functions

No.	TOE Security Function	
1	F.AUDIT	Audit log function
2	F.HDD_ENCRYPTION	HDD encryption function
3	F.ACCESS_DOC	Accumulated documents access control function
4	F.ACCESS_FUNC	User restriction control function
5	F.RIP	Residual information deletion function
6	F.I&A	Identification and Authentication function
7	F.SEPARATE_EX_INTERFACE	External interface separation function
8	F.SELF_TEST	Self-test function
9	F.MANAGE	Management function
10	F.SEUCRE_LAN	Network protection function

7.1 F.AUDIT (Audit log function)

F.AUDIT acquires audit log and also protects the acquired audit log against alteration and disclosure.

7.1.1 Audit log acquirement function

- Corresponding functional requirements: FAU_GEN.1, FAU_GEN.2

The TOE generates the following log.

Table 7-2 Audit Log

Events	Log
Start of Audit log acquirement function	Date/time of events Identification information of events Identification information of subjects Result of the events (Success or failure)
End of Audit log acquirement function	
Failure of login operation	
Authentication Suspension	
Recover from authentication suspension state	
Use of management function of Table 6-19	
Failure of communication through the network	
Change of time information	

7.1.2 Audit Log Review Function

- Corresponding functional requirements: FAU_SAR.1, FAU_SAR.2, FAU_STG.1

The TOE restricts reading and deletion of audit log only to U.ADMINISTRATOR with prohibiting the change of it. The TOE prevents the change of the audit log with providing the function of reading the audit log to client PC and deleting to U.ADMINISTRATOR

7.1.3 Audit storage function

- Corresponding functional requirements: FAU_STG.4(1) , FAU_STG.4(2)

The TOE stores the audit log in the HDD of the TOE, but the following process is performed when the storage area became full.

(1)When “Restriction of overwriting” is set,
the acceptance of jobs is suspended, and the audit log is not stored.

(2)When “Permission of overwriting” is set,
the oldest stored audit log is overwritten.

The settings of (1) and (2) are performed by U.ADMINISTRATOR.

7.1.4 Trusted time stamp function

- Corresponding functional requirements: FPT_STM.1, FMT_MTD.1

The TOE has clock function and provides U.ADMINISTRATOR with the function to modify TOE time. Only U.ADMINISTRATOR can change the time information by FMT_MTD.1. The TOE issues time stamp of clock function at the time of audit log generation and records as the audit log.

7.2 F.HDD_ENCRYPTION (HDD Encryption function)

- Corresponding functional requirements: FCS_CKM.1, FCS_COP.1, FIA_SOS.1(2)

The TOE performs encryption to protect data stored in HDD against unauthorized disclosure. Used encryption key and algorithm are as follows.

(1) Encryption Key

Encryption key is generated by Konica Minolta HDD encryption key generation algorism that Konica Minolta encryption specification standard defines. (Encryption key length is 256 bit.)

Unique encryption key for each TOE is generated by generating it based on the encryption passphrase set by U.ADMINISTRATOR. Only encryption passphrase that satisfies the following qualities is accepted.

- Number of characters: 20 characters
- Character type: possible to choose from 83 or more characters
- Rule:
  - ✧ Do not compose by only one and the same character.
  - ✧ Do not set the same value as the current setting after change.

(2) Encryption Algorithm

Encryption algorithm is shown in Table 7-3.

Table 7-3 Encryption Algorithm in HDD Encryption function

Encryption Key sizes	Encryption Algorithm
256 bit	Encryption algorithm which conforms to FIPS PUB197 (AES)

7.3 F.ACCESS_DOC (Accumulated documents access control function)

- Corresponding functional requirements: FDP_ACC.1(a), FDP_ACF.1(a)

The TOE accumulates documents in the Memory RX user box and Annotation user box. The access of accumulated documents are controlled by referring to the user box attributes (this is considered as the attribute of documents existing in the used box). And then, this can perform edit (rotate, delete of page, etc.), print, FAX TX, e-mail TX, etc.

The following shows the details of access control of documents in the user box.

Table 7-4 Operation of document in the System user box

User box		Operation of documents in the User box		
		Modify	read	Delete
Memory RX User Box	Saves FAX RX documents. sBOX PASSWORD is given to FAX RX documents.	X	box_passwd	box_passwd or U.ADMIN

Table 7-5 Details of Operation of document in the System user box

User box	Details of Operation of documents in the User box		
	Print	FAX RX	E-mail
Memory RX User Box	V	V	V

* U.ADMIN Represent that U. ADMINISTRATOR can operate.
box_passwd : Represent that only when password that matches to sBOX PASSWORD is input, it can be operated.

Table 7-6 Operation for documents in the function user box

User box		Operation to documents in User Box		
		modify	read	Delete
Annotation User Box	sBox PASSWORD is given to saved D.DOC	sbox_passwd	sbox_passwd	sbox_passwd or U.ADMIN

Table 7-7 Details of Operation for documents in the function user box

User box	Details of Operation of documents in the User box			
	Rotate	Print	FAX TX	E-mail TX
Annotation User Box	V	V	X	V

* U.NORMAL : Represent that U.NORMAL can operate.
U.ADMIN : Represent that U. ADMINISTRATOR can operate.
sbox_passwd : Represent that only when password that matches to sBOX PASSWORD is input, it can be operated.

Also, the access to the user box is prohibited when number of continuous mismatch of sBOX PASSWORD reached the administrator configurable positive integer within 1-3.

7.4 F.ACCESS_FUNC (User restriction control function)

- Corresponding functional requirements: FDP_ACC.1(a), FDP_ACF.1(a), FDP_ACC.1(b), FDP_ACF.1(b), FMT_MSA.1(b)

The TOE permits the operation of F.PRT, F.SCN, F.CPY, F.FAX and F.DSR, and the operation of Shared-medium interface necessary to it, according to the result of the comparison between Allocation Role of identified and authenticated user, and Permission Role of the function. Also, operation to Permission Role which is these attributes cannot be performed. Identified and authenticated user can perform only function that is permitted to oneself.

Also, following operations are available to D.DOC and D.FUNC (Except accumulated documents. Described in 7.3 about the accumulated documents) which occur during execution of functions.

Performed user is the user who has same User ID with the User ID of D.DOC and D.FUNC of operation objects.

-In case of PRINT

Following operations are possible

-Print

ID & Print user box, Password Encrypted PDF user box

U.NORMAL that performed that printing can print.

-Secure print user box

U.NORMAL that input the password that matches to the secure print password, set in the document, can print.

The access to the document (secure print) is prohibited when number of continuous mismatch of Secure print password reached the administrator configurable positive integer within 1-3.

-Preview

ID & Print user box

U.NORMAL that performed that printing can preview.

Secure print user box

U.NORMAL that input the password that matches to the secure print password,

set in the document, can preview.

-Delete

ID & Print user box, Password encrypted PDF user box

U.NORMAL and U.ADMINISTRATOR that performed that printing can delete.

Secure print user box

U.NORRMAL and U.ADMINISTRATOR that input the password that matches to the secure print password, set in the document, can delete.

-Edit of D.FUNC

ID & Print user box

U.NORMAL that performed that printing can perform edit of image shift and overlay.

-In case of SCAN

A preview is possible. Following operations are possible in the preview.

-Edit of D.FUNC

U.NORMAL that performed that scanning can rotate by page.

-Edit of D.DOC

U.NORMAL that performed that scanning can delete by page.

Scanned original data can be sent by e-mail and can be saved in user box. The waiting state of transmitting might occur, but in that case, the following operations are possible.

-Delete

U.NORMAL and U.ADMINISTRATOR that performed that scanning can delete the job that is waiting state of transmitting.

-In case of COPY

Following operations are possible.

- Print

U.NORMAL that performed that copying can print.

- Preview

U.NORMAL that performed that copying can preview.

Also, following operations are possible in the preview.

- Edit of D.FUNC

U.NORMAL that performed that copying can rotate the output by page.

- Delete

U.NORMAL and U.ADMINISTRATOR that performed that copying can delete the job.

-In case of FAX RX

U.USER can cancel FAX under receiving.

D.DOC received by FAX is saved in the user box.

-In case of FAX TX

A preview is possible. Following operations are possible in the preview.

-Edit of D.FUNC

U.NORMAL that performed that FAX TX can rotate by page.

-Delete

U.NORMAL and U.ADMINISTRATOR that performed that FAX TX can delete the job.

-Edit of D.DOC

U.NORMAL that performed that FAX TX can delete by page.

7.5 F.RIP (Residual information deletion function)

7.5.1 Temporary Data Deletion Function

- Corresponding functional requirement: FDP_RIP.1

The TOE prevents to reuse the residual information by overwriting and deleting the deleted document, the temporary document or its parts in HDD. This function is performed at the following timing.

(1) When a job such as print or scan is completed or suspended.
Delete the temporary document or its parts which is generated during job execution.

(2) When the deleting operation is performing.
Delete the specified document.

(3) When the residual information exists at the time of turning on the power.
When the power is turned off during deletion of (1) or (2) and the deletion was not completed with the residual information, this deletes them at the time of the power ON.

U.ADMINISTRATOR sets the overwriting data and the frequency of overwriting, by the operation setting function of the HDD data overwrite deletion function. The possible settings and its details are as follows.

Table 7-8 Operation Settings of Overwrite Deletion function of Temporary data

Setting	Contents (Overwritten data type and its order)
Mode:1	Overwrite once with 0x00
Mode:2	Overwrite with 0x00, 0xFF, 0x61 in this order and Verify the result.

7.5.2 Data Complete Deletion Function

- Corresponding functional requirements: FDP_RIP.1, FDP_ACF.1(a)

U.ADMINISTRATOR can perform overwriting and deleting to the data area including image data in HDD. This deletes document in HDD and prevents to reuse the residual information. U.ADMINISTRATOR sets the overwriting data and the frequency of overwriting, by the operation setting function of the HDD data overwrite deletion function. The possible settings and its details are as follows.

Table 7-9 Operation settings of Data Complete Deletion Function

Method	Overwritten data type and their order
Mode:1	0x00
Mode:2	Random numbers ⇒ Random numbers ⇒ 0x00

Method	Overwritten data type and their order
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

7.6 F.I&A (Identification and authentication function)

- Corresponding functional requirements: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1(1), FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FIA_USB.1, FTA_SSL.3

The TOE verifies that person who tries to use the TOE is the authorized user by using the identification and authentication information obtained from the user, and permits the use of the TOE only to the person who was determined as the authorized user. Identification and authentication function has the machine authentication method that the TOE itself identifies and authenticates, and the external server authentication method that uses external authentication server. When it is external server authentication method, it sends the input user ID to the external authentication server, and decrypts the returned credential by user key generated from input user password. If the decryption is succeed, authentication is successful, and the authentication is failed if the decryption failed.

The identification and authentication (except the time of print job input) is performed by selecting any of U.BUILTIN_ADMINISTRATOR, U.USER_ADMINISTRATOR or the other. The role is associated with the user if it's successful.

Table 7-10 Authentication method

Authentication method	Possible operations before success of identification and authentication	SFR
Machine Authentication External Server Authentication	Confirmation of suspension state of User use FAX RX Confirmation of TOE State and Setting of display, etc.	FIA_UID.1 FIA_UAU.1

* The setting of authentication method is performed by U.ADMINISTRATOR. Both Machine authentication and External sever authentication are activated at the same time. When both of them are activated, U.ADMINISTRATOR sets which methods are used for each user. User, who U.ADMINISTRATOR sets both authentication methods available, selects by oneself at the time of authentication.

The TOE also displays "*" for input password. FIA_UAU.7

When identification and authentication are successful, User ID, Allocation Role, and Role are combined to the process that acts as the appropriate user. FIA_ATD.1, FIA_USB.1

Moreover, the TOE prevents from setting the low strength password by restricting for

satisfying the following qualities in the passwords used for authentication.

Table 7-11 Password and Quality

Objective	Condition	SFR
Login Password	The TOE accepts only the password that satisfies the following. -Number of characters : 8 or more characters -Character type : possible to choose from 94 or more characters -Rule : (1) Do not compose by only one and the same character. (2) Do not set the same password as the current setting after change. Administrator sets the number of minimum characters. (must be more than 8 characters)	FIA_SOS.1(1)

When the authentication failed, the TOE performs the following process.

Table 7-12 Process at the time of authentication failure

Objective	Process	SFR
Authentication failure by login password	Authentication is suspended when number of continuous authentication failure reached the value that U.ADMINISTRATOR set. The number of authentication failure of U.NORMAL and that of U.USER_ADMINISTRATOR is totaled. If the user A tries to log in as U.NORMAL and failed (once), and successively the user A tries to log in as U.USER_ADMINISTROTOR and failed (once), the number of authentication failure of user A is two times. Authentication is also suspended even if the number of continuous authentication failure exceeds the setting value because of the change of setting value by U.ADMINISTRATOR. When the authentication of U.BUILTIN_ADMINISTRATOR is suspended, it is released by performing boot process of the TOE and passing the time set in the release time setting of operation prohibition for administrator authentication from boot process. In other cases, it is released by performing deletion function of number of authentication failure by U.ADMINISTRATOR, who is not in the authentication stopped state.	FIA_AFL.1

When there is no action of the identified and authenticated user for a certain period of time (setting time by administrator), the session is terminated. FTA_SSL.3

Table 7-13 Termination of interactive session

Objective	Session termination	Others
Operation panel	When it passes for the time determined by auto reset time, after processing of last	Auto reset time is set in the factory and administrator can change it.

	operation was completed.	
Web Connection	When it passes for the time determined by auto logout time, after processing of last operation was completed.	Auto reset time is set in the factory and administrator can change it.
Data Administrator	When it passes for 60 minutes, after processing of last operation was completed.*	Time is fixed
Printer driver Fax		There is no interactive session since accept of the request is the start and the completion of process is end. Identification and authentication is performed in each acceptance except Fax RX.

*This is the time considered the process that takes time such as downloading the registered information.

7.7 F.SEPARATE_EX_INTERFACE (External interface separation function)

- Corresponding functional requirement: FPT_FDI_EXP.1

The TOE prevents the access from telephone line by limiting the input information from telephone line to FAX RX and Remote Access function, and prohibits the direct transfer of received fax. Moreover, it is a structure which cannot be transfer the input from external interface including USB interface to Shared-medium Interface as it is.

7.8 F.SELF_TEST (Self-test function)

- Corresponding functional requirement: FPT_TST.1

The TOE contains the data for verification and decrypts it by using encryption passphrase when the power is ON. This verifies the integrity of encryption passphrase by confirming that the data for verification was decrypted correctly. And then, this provides HDD encryption function and the function to verify the normal operation. Moreover, the TOE verifies the integrity of TSF executable code by calculating hash value of control software when the power is ON and checking whether it corresponds to the recorded value or not. If the loss of completeness was detected in the integrity verification of encryption passphrase and control software, the TOE displays the alert on the operation panel and does not accept the operation.

7.9 F.MANAGE (Security management function)

- Corresponding functional requirements: FIA_SOS.1(1), FMT_MOF.1, FMT_MSA.1(a),

FMT_MSA.1(b), FMT_MSA.3(a), FMT_MSA.3(b), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

The TOE provides the following management functions.

Table 7-14 Management Function

Management function	Contents	Operator
Management function of Enhanced Security settings	Enable or disable Enhanced Security settings	U.ADMINISTRATOR
Management function of User Authentication function	Performs the setting of authentication method.	U.ADMINISTRATOR
Operation setting function of HDD data overwrite deletion function	Performs the operation setting of HDD data overwrite deletion function. (Setting of Mode)	U.ADMINISTRATOR
Audit log management function	Performs the operation setting when the audit log is full (Restriction of overwriting / Permission of overwriting). Read audit log and delete.	U.ADMINISTRATOR
Trust Channel Management Function	Communication Encryption Strength Setting (Change of communication encryption method)	U.ADMINISTRATOR
User management function	Registration and deletion of user to the TOE. Registration, modification and deletion of attributes (Authority) When it's External authentication method, user is registered in the TOE by using account password managed by the administrator at the time of first authentication.	U.ADMINISTRATOR
Initialization of attributes	The TOE initializes the security attributes of D.DOC and D.FUNC in accordance with Table 6 15. This initialization is performed at the generation of these objects and there is no function to interfere with this initializing process. The TOE also initializes the attributes of F.PRT, F.SCN, F.CPY, F.FAX and F.DSR in accordance with Table 6 16. This initialization is performed at the generation of these objects and there is no function to interfere	None

	with this initializing process.	
Registration function of U.NORMAL's login password	Register login password of U.NORMAL.	U.ADMINISTRATOR
Modification function of U.NORMAL's login password	Change login password of U.NORMAL	U.ADMINISTRATOR
	Change own password.	U.NORMAL
Modification function of U.BUILTIN_ADMINISTRATOR login password	Change own password. (About the U.BUILTIN_ADMINISTRATOR password, there is no setting function since initial value is set at factory default.)	U.BUILTIN_ADMINISTRATOR
Setting / Modification function of encryption passphrase	Set or change the encryption passphrase which is basic data for encryption key used for HDD encryption function.	U.ADMINISTRATOR
Modification function of Time information	Set the date and time information	U.ADMINISTRATOR
Modification function of Auto reset time	Change the Auto reset time. (There is no setting function since initial value is set at factory default.)	U.ADMINISTRATOR
Modification function of Auto logout time	Change the Auto logout time. (There is no setting function since initial value is set as factory default.)	U.ADMINISTRATOR
Modification function of Authentication failure frequency threshold	Change the threshold of the number of authentication failure. (There is no setting function since 3 is set as the initial value.)	U.ADMINISTRATOR
Registration / Modification function of External server authentication setting data	Register and change the setting data for the external authentication server (including the domain name that external server belongs to)	U.ADMINISTRATOR
Modification function of Release time of operation prohibition for Administrator authentication	Change the release time from prohibiting operation for Administrator authentication. (There is no setting function since initial value (5 minutes) is	U.ADMINISTRATOR

	set at factory default.)	
Deletion function of Password mismatch frequency	Delete the number of password mismatch. Accordingly, access prohibition of the user box is canceled	U.ADMINISTRATOR
Modification function of Password mismatch frequency threshold	Change the threshold of the number of password mismatch. (There is no setting function since 3 is set as the initial value.)	U.ADMINISTRATOR
Deletion function of Authentication failure frequency (except administrator)	Delete the number of authentication failure (except administrator). Accordingly, the lock of authentication function is canceled.	U.ADMINISTRATOR
Modification function of Password policy	Set and change Password policy.	U.ADMINISTRATOR
Registration / Modification function of Network setting	Set and change the network settings (IP address / port No. of SMTP sever / DNS server, MFP IP address, NetBIOS name, AppleTalk printer name, etc.)	U.ADMINISTRATOR
Registration / Modification function of transmission address	Register and change the transmission address setting (address of e-mail transmission, etc.)	U.ADMINISTRATOR
Management function of Object security attributes (except User ID, Box Type, DOC PASSWORD)	Change and delete the object security attributes (except User ID, Box Type, DOC PASSWORD).	U.ADMINISTRATOR
Management function of Subject security attributes (except object of management by user management function, sBOX PASSWORD, DOC PASSWORD)	Change and delete the subject security attributes (object of management by user management function, sBOX PASSWORD, DOC PASSWORD)	U.ADMINISTRATOR
Management function of Role	Add and delete U.USER_ADMINISTRATOR	U.ADMINISTRATOR

The management of Object security attribute is the deletion of object. If object is deleted, the attribute that is given to that object is also deleted.

Note that the operations of sBOX PASSWORD and DOC PASSWORD that are the subject security attributes, and the operations of User ID, Box Type, and DOC PASSWORD that are the object security attributes, are not available.

Table 7-15 Secure Print Password management function

Management function	Contents
Secure print password management function	The TOE accepts password only which satisfies the following as secure print password. Number of characters: 8 or more characters Character type: possible to choose from 94 or more characters Rule: Do not compose by only one and same character.

7.10 F.SECURE_LAN (Network communication protection function)

- Corresponding functional requirement: FTP_ITC.1

The TOE performs encryption communication in communications with IT devices. Encryption communication provided by the TOE is as follows. (When the Enhanced Security Setting is valid.)

Table 7-16 Encryption Communication provided by the TOE

Destination	Protocol	Encryption algorithm
Client PC	TLSv1.0,TLSv1.1,TLSv1.2	3DES(168 bits), AES(128bits, 256bits)
External authentication server	IPsec	3DES(168 bits), AES(128bits, 192bits, 256bits)
DNS server	IPsec	3DES(168 bits), AES(128bits, 192bits, 256bits)
SMTP server	IPsec	3DES(168 bits), AES(128bits, 192bits, 256bits)

---End---