bizhub PRESS C8000 Series

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

Security Target

Version: 1.17

Issued on: Oct. 07, 2010

Created by: KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

<Revision History>

Date	Ver.	Division	Approved	Checked	Created	Revision
2010/1/27	1.00	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Initial Version
2010/3/2	1.01	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Addition of TOE outline, addition of supplement to TOE description, correction of definition of audit target events, correction of description about threats (T.HDDACESS), and correction of other typographical errors
2010/3/12	1.02	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Correction of description about threats (T.HDDACESS), change of guidance name, and other typographical errors
2010/3/19	1.03	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Correction of description about assignment of FPT_TEE.1, and correction of other typographical errors
2010/3/24	1.04	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Correction of typographical errors
2010/4/6	1.05	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Correction along with deletion of FIA_UAU.6
2010/4/21	1.06	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Correction of typographical errors
2010/6/7	1.07	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Correction of description about audit log
2010/7/1	1.08	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Correction of typographical errors
2010/7/6	1.09	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Correction of typographical errors
2010/7/9	1.10	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Correction of typographical errors
2010/7/20	1.11	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Review of position of printer controller
2010/7/29	1.12	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Correction of typographical errors
2010/8/9	1.13	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Correction of typographical errors
2010/8/18	1.14	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Addition of description to OE.HDD

Date	Ver.	Division	Approved	Checked	Created	Revision
2010/9/13	1.15	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Review of description about threats
2010/9/29	1.16	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Review of description about threats, and addition of security policy of organization
2010/10/7	1.17	PP SW Development Division, Electronics Development Center, R&D Headquarters	Tetsuya Niijima	Yasuhiro Nakagami	Tomoo Kudo	Addition of information on controller

[Contents]

[List of Figures]

[List of Tables]

1. ST Introduction

1.1. ST Reference

- ST Title : The bizhub Press C8000 Series Security Target
- ST Version : 1.17
- Created on : Oct. 07, 2010
- Created by : KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

1.2. TOE Reference

- TOE Name : Japan bizhub PRESS C8000 Image Control Program
  Overseas bizhub PRESS C8000 Image Control Program
- TOE Version : A1RF0Y0-00I1-G00-10
- TOE Type : Software
- Created by : KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

1.3. TOE Overview

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

1.3.1. TOE Type

bizhub PRESS C8000 Image Control Program, which is TOE, is the embedded type software installed in the digital Multi Functional Peripheral “bizhub PRESS C8000” provided by KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

1.3.2. Usage of TOE and Main Security Functions

bizhub PRESS C8000 equipped with TOE is the digital Multi Functional Peripheral equipped with the network function, which provides the functions using the copy/printer functionality, the functions to operate and control bizhub PRESS C8000, and the functions to manage the maintenance of bizhub PRESS C8000 (hereinafter referred to as MFP collectively as the name for these functions). TOE is the "bizhub PRESS C8000 image control program" that executes the processing for operation control and the management of image data of which instructions issued from the panel of MFP body and through the network.

To prevent leakage of the highly confidential document data stored in the MFP, TOE, using the MFP, provides the function that identifies and authenticates a user who accesses the document data, and the access control function that gives the access permission to the document data only for the owner who has created the document data. TOE additionally implements the functions for various settings relevant to the behavior of security functions in the CE function, and the functions for management user numbers and passwords. The operation records of product users to TOE are stored being attached with time and date as the audit log, so that the administrator can detect unauthorized operations. In addition, HDDs (hard disk drives) that have the HDD lock function are equipped in the MFP, which are the media to store the document data. TOE sets the HDD passwords that conform to the prescribed password rules to the HDDs, checks the validity of the HDDs by the lock passwords at startup, and stops TOE and the MFP body operation if the validity is not confirmed.

1.4. TOE Description

1.4.1. Roles of TOE Users

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

- General user

  A general user who belongs to the organization that introduces the bizhub PRESS C8000 and uses the user functions related to copy and printer of the bizhub PRESS C8000. The general user can use the function to store the document on the HDD (Hard Disk Drive) of bizhub PRESS C8000 (the general user who is registered in TOE and can use the document data storage function is referred to as user).

  An ideal general user should have the basic knowledge of IT and be able to attack the network using the disclosed information but not able to develop a new undisclosed attack technique.

- Administrator

  An administrator should belong to the organization that introduces the bizhub PRESS C8000 and should manage the operations of the bizhub PRESS C8000. The administrator should use the operation control function provided by the bizhub PRESS C8000 to register the general user in TOE.

- Responsible person

  A responsible person should belong to the organization that introduces the bizhub PRESS C8000 and designate an administrator.

- CE[1]

  CE should belong to the company to which the maintenance of bizhub PRESS C8000 is consigned. CE should use the maintenance function provided by the bizhub PRESS C8000 to maintain it. CE should conclude the contract for maintenance of the bizhub PRESS C8000 with a responsible person or an administrator.

  In addition, general users, administrator, responsible person and CE are referred to as the product users.

[1] An Abbreviation of Customer service Engineer

1.4.2. Physical Scope of TOE

1.4.2.1. Use Environment

TOE is the image control software for the bizhub PRESS C8000. TOE installed bizhub PRESS C8000 is the digital multi-function products with network functions, which provide the functions utilizing copy and printer, functions for operation control of bizhub PRESS C8000, and functions for maintenance of bizhub PRESS C8000. An assumed office image as the use environments of bizhub PRESS C8000 is shown in "Figure 1 An example of the bizhub PRESS C8000 use environments".

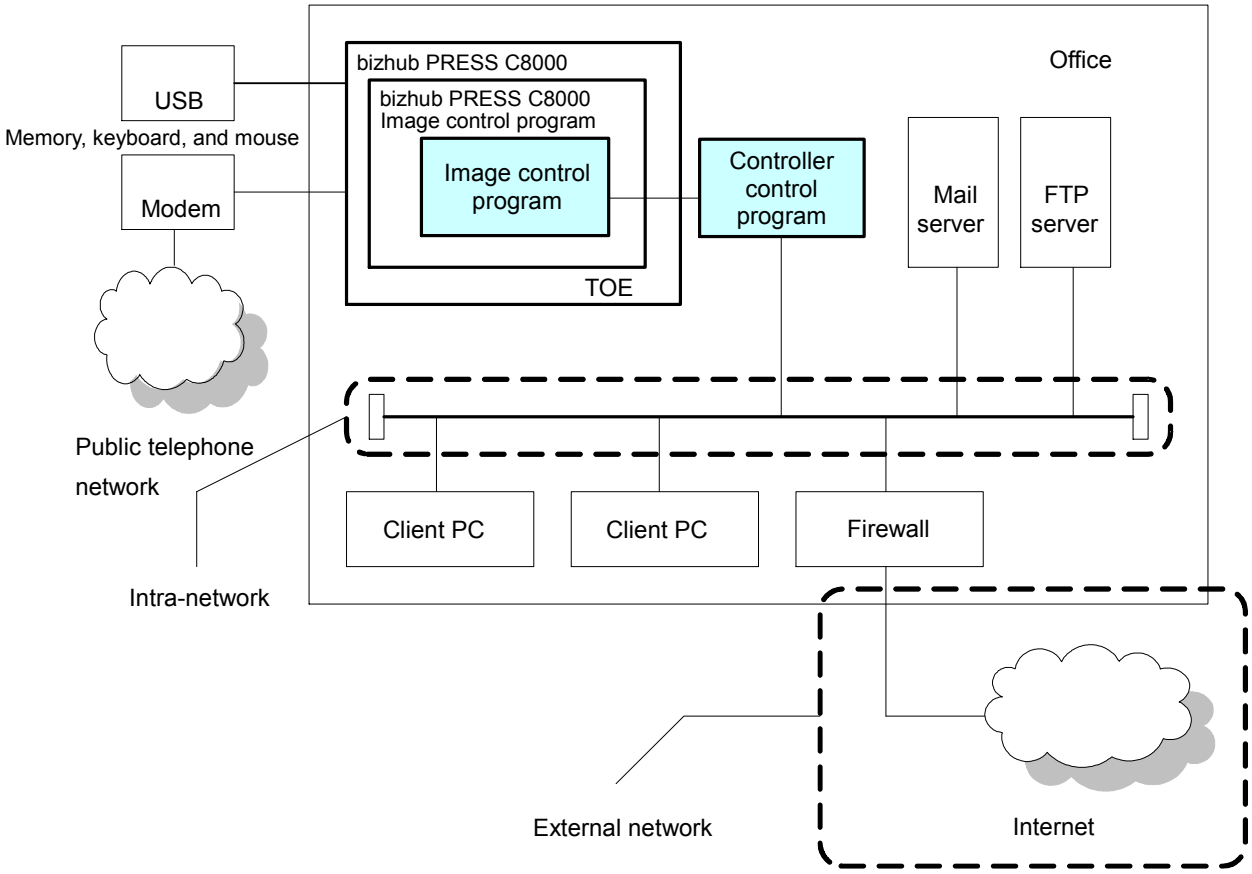

Figure 1 An example of the bizhub PRESS C8000 use environments

Intra-office LAN exists as the internal network of office. TOE has the means to connect the external network through the internal network but does not have the function to transmit/receive the document data. When the Enhanced Security Mode is activated (mentioned later), the functions used via the internal network are prohibited. TOE installed the bizhub PRESS C8000 is connected to the public telephone network and the USB Host interface as shown in “Figure 1 the bizhub PRESS C8000 use environments”. The public telephone network connected the MFP is used for the communication with CSRC. When the intra-office LAN connects to an external network, measures such as connecting via a firewall are taken, and an appropriate setup to block access requests to the MFP from the external network is applied to protect each device in the intra-network.

1.4.2.2. Operation Environment

"Figure 2 Hardware composition relevant to TOE" shows the structure of this TOE.

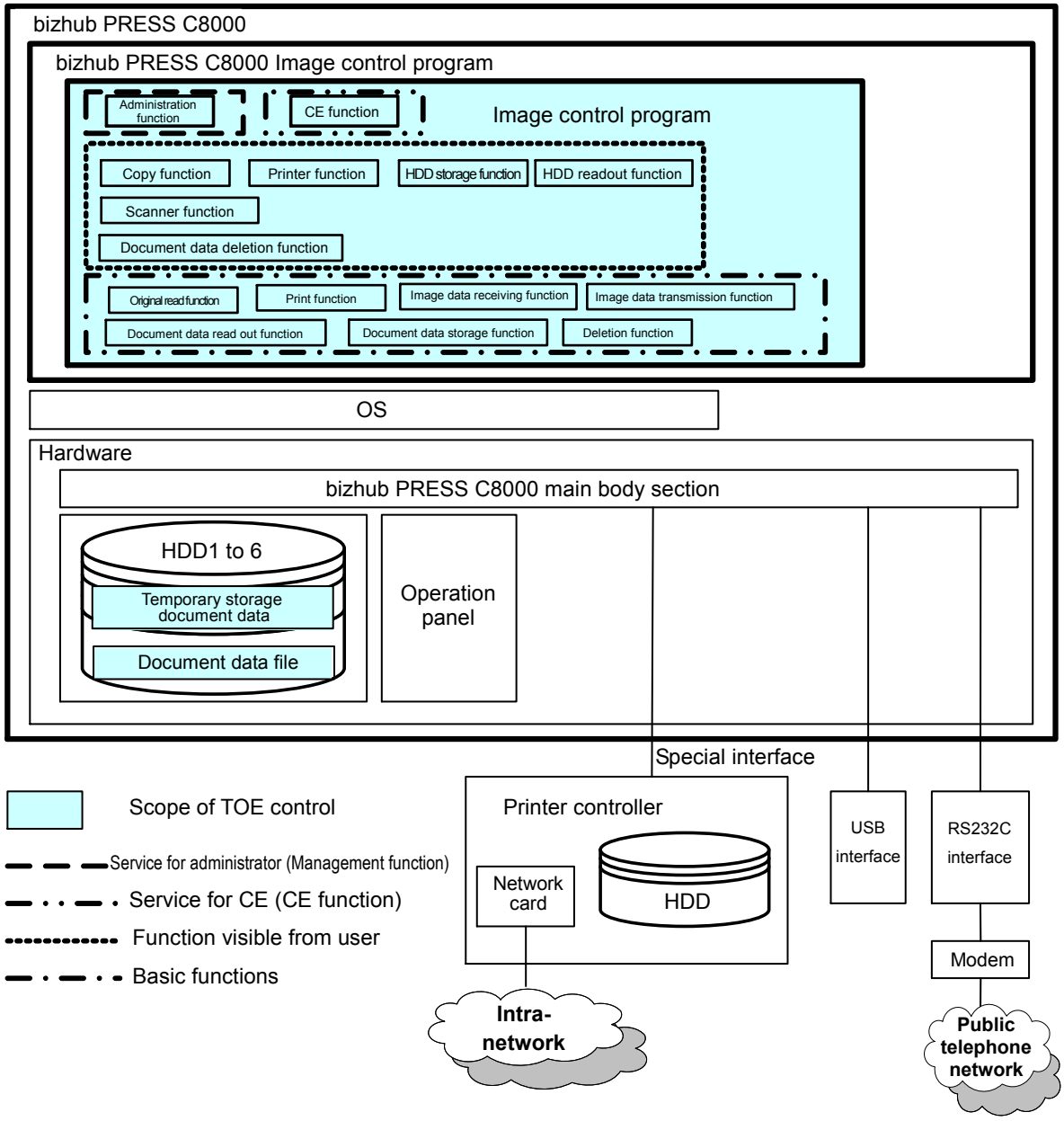

Figure 2 Hardware composition relevant to TOE

The bizhub PRESS C8000 consists of the hardware and the bizhub PRESS C8000 image control program. The hardware consists of the bizhub PRESS C8000 main body section, HDD1-6[2] section and operation panel. The bizhub PRESS C8000 main body section is equipped with the original read function to computerize the paper media document, print function to print the characters and graphics on the printing paper, image data receiving function to receive the image data from the printer controller[3], and image data transmission function to transmit the image data read by the original read

[2] The HDD1-6 section is equipped with the function (HDD lock function) that enables password setting and disabled to read and write when the password is invalid. This is not the standard part but the option part for MFP because of sales condition. However, this part is the essential component in the assumption of this ST.

[3] The controller control program is installed in the printer controller. The printer controller and the controller control program are the option parts and not required components in the assumption of this ST. Additionally, when the Enhanced Security Mode is activated

function of the printer controller. The UBS interface is the interface used for update of TOE and output of the audit log data, and it is disabled to access the document data via this interface. The HDD1-4 section has the storage devices that store the documents of each YMCK color and the temporary documents. The HDD5 section has the storage device that the image attribute data in the document data, and the image attribute data in the temporary document data. The HDD6 section has the storage device that stores the thumbnail of the document data. Document data of each YMCK color, image attribute data, and thumbnail are referred to as document data collectively. The bizhub PRESS C8000 image control program works on OS. OS controls the hardware and input-output of the document data from/to the bizhub PRESS C8000 image control program. The image control program controls the management function, CE function, user functions (that indicates the copy function, printer function, Scan to Email function, Scan to FTP function, Scan to PC (SMB) function, HDD storage function, HDD readout function, and document data deletion function as shown in Table 1 Correspondence between User Functions and Basic Functions), and the basic functions (such as original read function, print function, deletion function, document data storage function, document data readout function, image data receiving function, and image data transmission function).

The document data is created on the storage devices of HDD1-6 along with the operation of the bizhub PRESS C8000 image control program. Folders can be created on the HDD1-6, where document data can be stored. The scope of TOE control is the hatching area of “Figure 3 Hardware composition relevant to TOE”.

The bizhub PRESS C8000 accepts the processing requests from the product user via the operation panel and the processing requests from the product user via the controller connected with the special interface, and TOE executes such processing.

1.4.2.3. Guidance

- bizhub PRESS C8000 User's Guide Copier(Japanese version)
- bizhub PRESS C8000 User's Guide Main Body(Japanese version)
- bizhub PRESS C8000 User's Guide Network Scanner(Japanese version)
- bizhub PRESS C8000 User's Guide Security(Japanese version)
- bizhub PRESS C8000 SERVICE MANUAL(Japanese version)
- bizhub PRESS C8000 INSTALLATION MANUAL(Japanese version)
- bizhub PRESS C8000 User's Guide Copier
- bizhub PRESS C8000 User's Guide Main Body
- bizhub PRESS C8000 User's Guide Network Scanner
- bizhub PRESS C8000 User's Guide Security
- bizhub PRESS C8000 SERVICE MANUAL
- bizhub PRESS C8000 INSTALLATION MANUAL

1.4.3. Logical Scope of TOE

Users use a variety of functions of TOE from the panel. Hereinafter, this section explains typical functions such as basic function, management function manipulated by administrators, and CE function manipulated by service engineers (hereinafter referred to CE).

(mentioned later), its relevant printer controller is the one that is embedded. With inquires regarding the relevant printer controller, contact the retail store.

1.4.3.1. Basic Function

As shown in "**Table 1 Correspondence between User Functions and Basic Functions**", the user functions are achieved by execution of the basic functions. The following paragraphs explain the basic functions.

Table 1 Correspondence between User Functions and Basic Functions

No	User function	Basic function
1	Copy function	Original read function and print function
2	Printer function	Image data receiving function and print function
3	Scanner functions (Scan to Email function, Scan to FTP function, and Scan to PC (SMB) function)	Original read function and image data transmission function
4	HDD storage function	Original read function or image data receiving function, and document data storage function
5	HDD readout function	Document data readout function and print function
6	Document data deletion function	Deletion function

"Figure 3 Basic function processing flow diagram" shows the processing flow reliant to the user function and the basic function shown in Table 1.

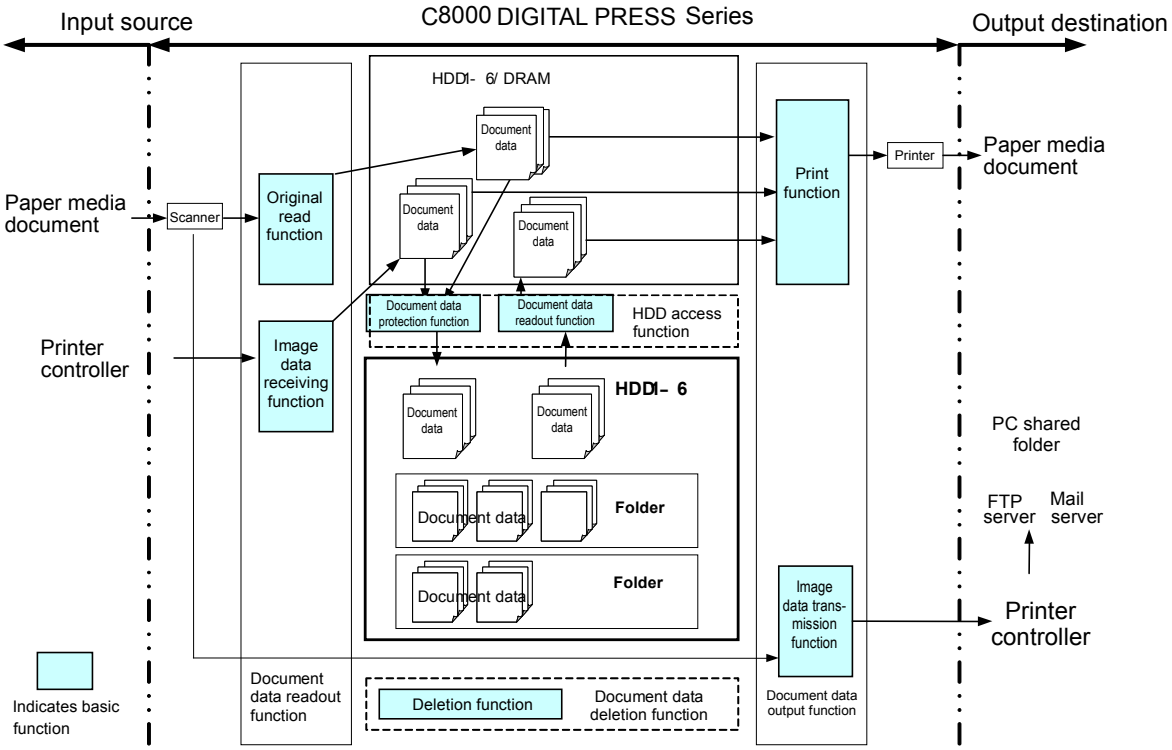

Figure 3 Basic function processing flow diagram

The following paragraphs explain the functions shown in "Figure 3 Basic function processing flow diagram".

(1) Original read function

This function imports the information on paper media document from the scanner, which is instructed by a general user from the operation panel, and converts the information to the document data. The converted data is stored in HDD1-6 or DRAM temporarily.

(2) Image data receiving function

This is the function to store the document data transmitted from the printer controller in HDD1-6 or DRAM temporarily. This function is valid only when the printer controller (option part) is equipped.

(3) Document data storage function

This is the function to store the document data that was temporarily stored in HDD1-6.

(4) Document data readout function

This is the function to read out the stored document data from HDD1-6.

(5) Print function

This is the function to print the document data that was temporarily stored in HDD1-6 or DRAM.

(6) Image data transmission function

This is the function to transmit the document data imported using the original read function to the printer controller. This function is valid only when the printer controller (option part) is equipped.

(7) Deletion function

This is the function to delete the document data stored temporarily or permanently.

The followings are the security functions provided from TOE.

- Identification and authentication function

TOE identifies and authenticates a user using a user ID and a user password, and gives the permission for user to modify the user password and access the stored document data after identification-authentication succeeds.

- Access control function

TOE can limit the users who can access the stored document data. The access control function permits only the valid users authenticated to read out the own document data.

- Audit function

TOE can keep a log of audit trails for the security function behavior. The following events are created as the audit logs: success/failure in identification-authentication of CE and administrator identities, success of modification of HDD lock password, success of enhanced security mode setting (activation/stop), readout and print of document data, readout and print of audit logs and output of audit logs to USB, and time stamp (YY/MM/DD/hh/mm/ss) for each operation event at

occurrence of operations associated with management functions for registration/modification/ deletion and description of each operation.

1.4.3.2. Management Function

TOE provides the functions such as the management of various settings, e.g. for enhanced security mode, in the administrator mode that only an authenticated administrator can manipulate from the panel. The administrator executes various operations settings of the functions of TOE using the management function. The administrator uses the management function to manage the information relevant to the operation of digital multi-function product such as creation of user/modification of user password, print of audit information, administration of printer count, troubleshooting, toner management, etc.

The following shows the functions related to the security.

- User management
  - Registration or modification of user No.
- Setup of HDD lock function
  - Modification of HDD lock password

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

- Setup of enhanced security mode
  - Stop

1.4.3.3. CE Function

TOE provides a management function of administrator and a maintenance function, such as adjusting the device for Scan/Print etc, within the service mode that only CE can operate. The CE also accesses the bizhub PRESS C8000 from a computer connected to the public telephone network or a computer connected to the internet to acquire the information on such as printer count, jam count, toner shortage, etc. for hardware maintenance. (CS Remote Care, hereinafter, abbreviated to CSRC. Refer to "1.4.3.6".) CSRC is performed via the RS232C interface, E-Mail interface or HTTP interface. Note that a unique communication protocol, i.e. a unique transfer standard for the modem, is used for the RS232C interface, and also unique message communication protocol is used for the E-Mail interface and the HTTP interface. This CSRC does not have any interface to the document data and also cannot execute the security related functions.

The followings are the major functions related to security.

- Registration and modification function of administrator password
- Modification function of CE password

The following is a set of operation setting functions that have influence especially to the behavior of the security function.

- Authentication setup of CE with the CE password

- Select "Stop".

1.4.3.4. Other Functions

TOE makes effective use of the HDD lock function of HDD, which is an external entity. The following explains the typical functions related to the external entity.

- Test function of HDD lock system

HDD, an external entity, has the measure against data leakage, etc, due to connection to an irregular device, of which HDD lock function is implemented and activated effectively by setting a password. TOE utilizes the HDD lock function that enables to activate the HDDs (HDD1-6) only when authentication by a HDD lock password succeeds and stop the operation of HDD when authentication fails.

1.4.3.5. Enhanced Security Function

Various setting functions related to the behavior of the security function for the Management function and the CE function can be set collectively to the secure values by the operation settings of the "Enhanced Security Function". Each value set is prohibited modifying itself into the vulnerable one individually.
The following explains the series of the setting condition of being the enhanced security mode active. In order to activate the enhanced security mode, the prerequisite is required that an administrator password and a CE password should be set along with the password policy.

- User identification authentication function : Active
- CE authentication function : Active
- Password policy function[4] : Active
- Audit function : Active
- CSRC function (Modem) : Active
- CSRC function (Mail/Http) : Prohibited
- TOE update function via USB : Active
- Network management function : Prohibited
- TOE update function via Internet : Prohibited
- Non-volatile storage function : Prohibited
- HDD backup/restore : Prohibited
- Set data readout/storage function : Prohibited

1.4.3.6. Terminology

The table bellow defines the terminologies used in this ST.

[4] When the password policy function is active, all the registration and modification of user passwords of less than 8 digits are rejected.

No.	Terminology	Explanation
1	Document data	Document data is the data that the information such as characters and graphics is digitized.
2	Paper media document	Paper media document is the paper media-based document containing characters and graphics.
3	Operation panel	Operation panel is the collective name for the touch panel and the operation buttons which is attached to the enclosure of the bizhub PRESS C8000.
4	Intra-network	Intra-network is the LAN of organization that introduces the bizhub PRESS C8000, to which client PCs and various servers (e.g. Mail Server and FTP Server).
5	External network	External network is the network other than the intra-network (refer to No.5) (e.g. Internet).
6	SMB	SMB is the application protocol for communications between computers on the Microsoft system OS.
7	User	General user whose user identifier (user No.) and user password are registered in TOE by the administrator, and who possesses own document data on the HDD (hard disk drive) of the bizhub PRESS C8000
8	CSRC	CSRC is the application that implements the CS Remote Care function. This function notifies occurrence of MFP troubles to the center terminal PC allocated in the service base and notifies the counter information and others responding to the request from the center terminal PC. The RS232C interface, E-Mail interface, or HTTP interface are used for such communication, but only the RS232C interface (modem) is permitted to use if the enhanced security mode is active.
9	Network management function	This is the function that is enabled after successful identity authentication of administrator via a network, which consists of the internet ISW function (the function to rewrite TOE from an external server via the Internet), WEB tool (the function to acquire the setting information of product main body and execute the management function via the intra-network), and output history logging function (the function with the main body to output the output JOB history to a connected external PC via NIC). All the functions are disabled when the enhanced security mode is active.

2. Conformance Claims

2.1. CC Conformance Claim

This ST conforms to the following standards.

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model Version 3.1 Revision 3 (Japanese Translation v1.0)
Part 2: Security functional components Version 3.1 Revision 3 (Japanese Translation v1.0)
Part 3: Security assurance components Version 3.1 Revision 3 (Japanese Translation v1.0)

- Security functional requirement: Part 2 Conformant
- Security assurance requirement: Part 3 Conformant

2.2. PP Claim

There is no PP that is referenced by this ST.

2.3. Package Claim

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

3. Security Problem Definition

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

3.1. Protected Assets

The assets to be protected by TOE are the document data sets in the hard disks (HDD1-6) of the bizhub PRESS C8000, and TOE prevents leakage of the document data.

The original data of document data that is owned by a user in a client PC or as the paper media and still not stored in HDD of the MFP is not protected.
Also the document data in DRAM that is stored temporarily in DRAM in the process of document data processing is not protected. (* The document data temporarily stored in DRAM is not exposed to the threat of data leakage, because access to DRAM from an external device is impossible and the data temporarily stored in DRAM is erased at power OFF.)

3.2. Assumptions

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

ASM.SECMOD (Setting conditions of enhanced security mode)
An administrator activates the enhanced security mode.

ASM.PLACE (Installation conditions of TOE)
TOE should be installed in the area where only the product users can operate it.

ASM.NET (Installation conditions of intra-network)
When the intra-network where the bizhub PRESS C8000 with TOE was installed is connected to an external network, access from the external network to the bizhub PRESS C8000 is not allowed.

ASM.ADMIN (A reliable administrator)
An administrator is not a person who never misbehaves.

ASM.CE (Conditions of CE)
CE is not a person who never misbehaves.

ASM.SECRET (Operational condition about secret information)
In the use of TOE, the administrator password and HDD lock password should not be leaked from the administrator. Also the CE password should not be leaked from CE and the user password should not be leaked from a user.

ASM.SETTING (Operational setting conditions about security)
- Activates setting of HDD lock function.
- Activates login authentication of CE.

3.3. Threats

In this section, threats that are assumed during the use of TOE and the environment for using TOE are identified and described.

T.ACCESS (Unauthorized access to document data)

When a general user uses the user function through the operation panel, there is a threat of leakage of document data that are owned by the other general users.

T.IMPADMIN (Impersonation to CE or administrator)

There is a threat of data leakage of document data with malicious intent access by a general user through the CE function interface and the management function interface.

3.4. Organizational Security Policies

In this section, organizational security policies that are assumed during the use of TOE and the environment for using TOE are identified and described.

P.CHECK-HDD (Verification of HDD)

TOE verifies the HDD with the lock password of HDD and also limits the management of lock password of HDD to the administrator. TOE accepts only the 8 to 32 digits of half size upper case alphabets, half size lower case alphabets and half size numbers as the HDD lock password.

4. Security Objectives

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

4.1. Security Objectives for TOE

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

O.IA (Identification and authentication)

TOE identifies and authenticates the user, administrator, and CE who intend to access TOE. The user can modify own user password after identification and authentication are completed successfully.

O.ACCESS (Access limitation)

TOE permits only the user who is identified and authenticated to access the stored document data created by that user.

O.MANAGE (Provision of management function)

TOE permits only the administrator to operate the following functions.

- Functions related to settings of the enhanced security mode
- Functions to register and modify the user password
- Functions to register and modify the user No.
- Modification of the HDD lock password

TOE permits only CE the operation of the following functions.

- CE password registration and modification functions
- Administrator password registration function

TOE permits the administrator and CE to operate the following functions.

- Administrator password modification function

TOE accepts only the 8 to 32 digits of half size upper case alphabets, half size lower case alphabets and half size numbers as the HDD lock password.

O.AUDIT (Audit information log)

TOE stores the audit log when the access event to the assets to be protected and relevant events occur in TOE. The audit log records the date and time at time of event occurrence, type of event, and result of event. In addition, TOE limits the permission of reference to the audit information to the administrator and CE. TOE assures to keep the audit logs equivalent to the disk capacity by overwriting the oldest stored audit log with the latest audit log when the area for output of the audit log reaches its set capacity.

O.CHECK-HDD (Verification of HDD)

TOE stops the operation of TOE and MFP main body when authentication of the HDD lock password for HDD (HDD1-6) fails.

4.2. Security Objectives for the Operational Environment

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

OE.ADMIN (A reliable administrator)

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

OE.SERVICE (CE's guarantee)

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

OE.PLACE (Management of installing location)

The administrator installs TOE at a compartment where only the product users can operate.

OE.SECOND (Settings of enhanced security mode)

The administrator activates the enhanced security mode.

OE.NET (Management of network)

The administrator carries out the measures for the unauthorized access from the outside by setting up the equipment such as the firewall to intercept the access from an external network to MFP with TOE.

OE.HDD (Protection of HDD)

The administrator and CE install the HDDs (HDD1-6) with the HDD lock function to the MFP and set the functions to use the HDDs.

OE.SESSION (Termination of session after operation)

The administrator has the user implement the following operation.

- The user executes the logoff operation after the operation for the document data.

The administrator executes the following operation.

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

The CE executes the following operation.

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

OE.SECRET (Appropriate management of confidential information)

The administrator executes the following operation.

- The administrator educates the user not to leak own user password to the others.
- Keep the administrator password and HDD lock password confidential.
- Modify the administrator password and HDD lock password appropriately.

The CE executes the following operation.

- Keep the CE password confidential.
- Modify the CE password appropriately.

- When the CE modifies the administrator password, make the administrator modify it promptly.

OE.SETTING-SECURITY (Operational setup for security)

- The administrator makes the HDD lock function (for HDD1-6) "active".
- The administrator makes the CE authentication function "active" with CE.

4.3. Security Objectives Rationale

4.3.1. Necessity

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

Table 2 Conformity of Security Objectives to Assumptions, Threats, and Organization Security Policies

Security objectives \ Organization security policies / Assumptions / Threats	ASM.SECMOD	ASM.PLACE	ASM.NET	ASM.ADMIN	ASM.CE	ASM.SECRET	ASM.SETTING	T.ACCESS	T.IMPADMIN	P.CHECK-HDD
O.IA								●	●	●
O.ACCESS								●		
O.MANAGE								●	●	●
O.AUDIT								●	●	●
O.CHECK-HDD										●
OE.ADMIN				●						
OE.SERVICE					●					
OE.PLACE		●								
OE.SECOND	●									
OE.NET			●							
OE.HDD										●
OE.SESSION								●	●	
OE.SECRET						●				
OE.SETTING-SECURITY							●			

4.3.2. Sufficiency of Assumptions

The security objectives for the assumptions are described as follows.

- **ASM.SECMOD (Enhanced security mode setup condition)**
  This condition assumes that the administrator activates the enhanced security mode.
  OE.SECOND specifies that this is used after the administrator activates the enhanced security mode, so that this condition is realized.

- **ASM.PLACE (Conditions for TOE installation)**
  With OE.PLACE, TOE is installed in the area where only the product users can operate it.
  Consequently, the access to TOE can be limited only to the product users.
  As described above, the assumptions ASM.PLACE is realized with the security objective

OE.PLACE.

- **ASM.NET (Intra-network setup condition)**
  This condition assumes that there is no access by an unspecified person from an external network to the intra-network.
  OE.NET specifies the unauthorized access prevention from external by the installation of devices such as firewall in order to block access to the MFP from the external networks, so that this condition is realized.

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

- **ASM.CE (Conditions for CE)**
  This condition assumes CE is not malicious.
  With OE.SERVICE, the organization that manages the maintenance of the MFP educates CE. Also the administrator needs to observe the maintenance of the MFP, so that the reliability of CE is assured.

- **ASM.SECRET (Operating condition concerning confidential information)**
  This condition assumes each password using for the use of TOE should not be leaked by each user.
  OE.SECRET specifies that the administrator makes the user to execute the operation rule concerning the user password and that the administrator executes the operation rule concerning the administrator password and HDD lock password. It also specifies that CE executes the operation rule concerning the CE password, and that CE makes the administrator to execute the operation rule concerning the administrator password, so that this condition is realized.

- **ASM.SETTING (Operational setup condition concerning security)**
  This condition assumes the following settings that satisfy the operational setup conditions for security to TOE.
  - Activation of the HDD lock function by the administrator
  - Activation of the CE authentication function

  OE.SETTING-SECURITY specifies that the above conditions should be set to all the items described above, so that this condition is realized.

4.3.3. Sufficiency of Threats

The security objectives against threats are described as follows.

- **T.ACCESS: Unauthorized access to document data**
  This threat assumes the possibility that the document data of other general user leaks through use of the user function by a general user.
  With O.MANAGE, TSF permits only the proper administrator identified and authenticated by O.IA to use the user No. registration/deletion function and the administrator determines the user who can use the document data using this function. The enhanced security mode is kept in the active status

during operation by limiting the setup of enhanced security mode only to the administrator, and the strength of user password is ensured by activation of the user identification-authentication function and the password policy function. TSF permits only the proper user identified and authenticated through O.IA to read out the document data with O.ACCESS.
Since TOE records the operations for the user function to the document data that is the "assets of protection objects" as the audit information with O.AUDIT, it is possible to detect unauthorized operations to the document data.
Since logout is executed without fail after the operations for CE, administrator and user with OE.SESSION, no ones other than MFP operators can operate the MFP in the authenticated status.
Thus, the sufficiency of threat T.ACESS is assured sufficiently with the security objectives O.IA, O.ACCESS, O.MANAGE, O.AUDIT, and OE.SESSION.

- **T.IMPADMIN: Impersonation to CE or administrator**

Such possibility is assumed for this threat that a general user impersonates CE or administrator to leak the document data.
TSF identifies and authenticates a CE with O.IA. The CE who is identified and authenticated with O.MANAGE registers the administrators selected by the responsible person of the organization that manages the MFP, and makes the status of management function enable to only the administrators who are identified and authenticated.
Additionally, with O.AUDIT, TSF enables to detect the trace of operations for impersonation to CE or administrator to record the events of registration and modification of CE or administrator passwords as the audit information.
Since logout is executed without fail after the operations for CE and administrator with OE.SESSION, no ones other than MFP operators can operate the MFP in the authenticated status.
Thus, the sufficiency of threat T.IMPADMIN is assured sufficiently with the security objectives O.IA, O.MANAGE, O.AUDIT, and OE.SESSION.

4.3.4. Sufficiency of Organizational Security Policies

Security objective corresponding to organizational security policies is explained as follows.

- **P.CHECK-HDD: Verification of HDD**

The TFS modifies and manages the HDD lock passwords of HDD1-6 with the management function of O.MANAGE by the valid administrator who is identified and authenticated with O.IA. O.MANAGE accepts only the 8 to 32 digits of half size upper case alphabets, half size lower case alphabets and half size numbers as the HDD lock password.
The enhanced security mode is always kept in the active status during operation by limiting the enhanced security mode setting only to the administrator, and the HDD lock function is activated. Additionally the TSF enables to detect the modification attempts to modify the function setting related to the HDD password by a person who impersonates to the administrator because O.AUDIT records the unsuccessful administrator identification-authentication events, successful enhanced security mode setting events, successful HDD lock password modification events as the audit information. Also by O.CHECK-HDD, it stops the operation of TOE and the MFP main body when authentication of the HDD lock password for HDD1-6 fails.
OE.HDD indicates that the HDDs (HDD1-6) with the HDD lock function shall be installed in MFP.
Thus, the organization security objectives P.CHECK-HDD is achieved with O.IA, O.MANAGE, O.AUDIT, O.CHECK-HDD, and OE.HDD.

5. Extended Components Definition

This ST does not define extended components.

6. IT Security Requirements

In this chapter, TOE security requirements are described.

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

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

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

6.1. TOE Security Requirements

6.1.1. TOE Security Functional Requirements

6.1.1.1. Audit

FAU_GEN.1	**Audit data generation**
FAU_GEN.1.1	
The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and c) [assignment: *other specifically defined auditable events*].	
[selection, choose one of: *minimum, basic, detailed, not specified*] ***No specification***	
[assignment: *other specifically defined auditable events*] ***Following audit target events*** ***- Successful/unsuccessful identification and authentication at the identification and authentication of CE*** ***- Successful/unsuccessful identification and authentication at the identification and authentication of administrator*** ***- Successful/unsuccessful identification and authentication at the identification and authentication of user*** ***- Successful settings of the enhanced security mode*** ***- Successful print of the audit log*** ***- Successful output of the audit log to USB*** ***- Successful modification/registration of the CE password*** ***- Successful modification/registration of the administrator password by CE*** ***- Successful modification of the administrator password by administrator*** ***- Successful modification/registration of the user password by the administrator***	

- Successful deletion of the user No. by the administrator -Successful of modification of the user password by the user - Modification of the HDD lock password - Successful readout and print of the document data -Successful registration of the user No. by the administrator	
FAU_GEN.1.2	
The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].	
[assignment: *other audit relevant information*] ***None***	
Hierarchical to :	No other components
Dependencies :	FPT_STM.1

Table 3 Auditable Events

Functional requirements	Auditable events defined by CC	Auditable events
FAU_GEN.1	There are no auditable events foreseen.	None
FAU_STG.1	There are no auditable events foreseen.	None
FAU_STG.4	Basic: Actions taken due to the audit storage failure.	None (Reason: TOE stops when audit storage fails.)
FAU_SAR.1	Basic: Reading of information from the audit records.	Successful audit log print Successful output of the audit log to USB
FAU_SAR.2	Basic: Unsuccessful attempts to read information from the audit records.	None (Reason: Access to the audit log is possible from only the administrator usable administrator mode.)
FDP_ACC.1	There are no auditable events foreseen.	None
FDP_ACF.1	a) Minimal: Successful requests to perform an operation on an object covered by the SFP. b) Basic: All requests to perform an operation on an object covered by the SFP. c) Detailed: The specific security attributes used in making an access check.	Successful readout and print of the document data
FIA_AFL.1	Minimal: 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).	Arrival at the threshold value for unsuccessful authentication of the administrator, CE, and user
FIA_ATD.1	There are no auditable events foreseen.	None
FIA_SOS.1[1]	a) Minimal: Rejection by the TSF of any tested secret; b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of any changes to the defined quality metrics.	Successful registration/modification of the CE password
FIA_SOS.1[2]	a) Minimal: Rejection by the TSF of any tested secret; b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of any changes to the defined quality metrics.	Successful registration/modification of the administrator password
FIA_SOS.1[3]	a) Minimal: Rejection by the TSF of any tested secret; b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of any changes to the defined quality metrics.	Successful registration/modification of the user password

Functional requirements	Auditable events defined by CC	Auditable events
FIA_SOS.1[4]	a) Minimal: Rejection by the TSF of any tested secret; b) Basic: Rejection or acceptance by the TSF of any tested secret; c) Detailed: Identification of any changes to the defined quality metrics.	Successful modification of the HDD lock password
FIA_UAU.2[1]	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism.	Successful and unsuccessful authentication at the authentication of CE
FIA_UAU.2[2]	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism.	Successful and unsuccessful authentication at the authentication of administrator
FIA_UAU.2[3]	a) Minimal: Unsuccessful use of the authentication mechanism; b) Basic: All use of the authentication mechanism.	Successful and unsuccessful authentication at the authentication of user
FIA_UAU.7	There are no auditable events foreseen.	None
FIA_UID.2[1]	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	Successful and unsuccessful authentication at the identification of CE
FIA_UID.2[2]	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	Successful and unsuccessful authentication at the identification of administrator
FIA_UID.2[3]	a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; b) Basic: All use of the user identification mechanism, including the user identity provided.	Successful and unsuccessful authentication at the identification of user
FIA_USB.1	a) Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject). b) Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	Successful generation of a subject
FMT_MOF.1	Basic: All modifications in the behaviour of the functions in the TSF.s	Successful termination of the enhanced security mode
FMT_MSA.3	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.	None (Reason: the security attributes initial values are normally fixed and cannot be modified.)
FMT_MTD.1[1]	Basic: All modifications to the values of TSF data.	Successful registration of the user No. by the administrator Successful registration of the user password by the administrator
FMT_MTD.1[2]	Basic: All modifications to the values of TSF data.	Successful modification of the user password by the administrator Successful modification of the user password by the user
FMT_MTD.1[3]	Basic: All modifications to the values of TSF data.	Successful modification of the administrator password
FMT_MTD.1[4]	Basic: All modifications to the values of TSF data.	Successful modification of the CE password
FMT_MTD.1[5]	Basic: All modifications to the values of TSF data.	Successful registration of the administrator password Successful registration of the CE password
FMT_MTD.1[6]	Basic: All modifications to the values of TSF data.	Successful modification of the HDD lock password

Functional requirements	Auditable events defined by CC	Auditable events
FMT_MTD.1[7]	Basic: All modifications to the values of TSF data.	Successful deletion of user No.
FMT_SMF.1	Minimal: Use of the management functions.	Successful settings of the enhanced security mode Successful registration of the user No. by the administrator Successful deletion of the user No. by the administrator Successful registration of the user password by the administrator Successful modification of the user password by the administrator Successful modification of the HDD lock password by the administrator Successful modification of the user password by the user Successful registration of the administrator password by the administrator Successful modification of the CE password by CE Successful modification of the administrator password by CE
FMT_SMR.1[1]	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.	None (Reason: the rolls of CE are fixed.)
FMT_SMR.1[2]	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.	None (Reason: the rolls of administrator are fixed.)
FMT_SMR.1[3]	a) Minimal: modifications to the group of users that are part of a role; b) Detailed: every use of the rights of a role.	None (Reason: the rolls of user are fixed.)
FPT_STM.1	a) Minimal: changes to the time; b) Detailed: providing a timestamp.	None (Reason: unnecessary because the time setting is disabled when the enhanced security mode is valid.)
FPT_TEE.1	Basic: Execution of the tests of the external entities and the results of the tests.	None (Reason: TOE is not activated if the HDD lock password authentication fails.)

FAU_STG.1	**Storage of protected audit trail**
FAU_STG.1.1	
The TSF shall protect the stored audit records in the audit trail from unauthorised 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*] ***Protection***	
Hierarchical to :	No other components
Dependencies :	FAU_GEN.1

FAU_STG.4	Protection of audit data loss
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.	
[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"*] ***Overwriting the oldest audit log stored***	
[assignment: *other actions to be taken in case of audit storage failure*] ***None***	
Hierarchical to :	FAU_STG.3
Dependencies :	FAU_STG.1

FAU_SAR.1	Audit review
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*] ***Administrator and CE***	
[assignment: *list of audit information*] ***Audit information indicated in "Table 3 Auditable Events" specified in FAU_GEN.1***	
FAU_SAR.1.2	
TSF shall provide the user with the audit log in a format that is suitable for interpretation of that information.	
Hierarchical to :	No other components
Dependencies :	FAU_GEN.1

FAU_SAR.2	Limited 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.	
Hierarchical to :	No other component
Dependencies :	FAU_SAR.1

6.1.1.2. User data protection

FDP_ACC.1	Subset access control
FDP_ACC.1.1	
The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].	
[assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]: ***Listed in "Table 4 Document Data Access Control: Operational List"***	
[assignment: *access control SFP*]: ***Document data access control***	
Hierarchical to :	No other components
Dependencies :	FDP_ACF.1

Table 4 Document Data Access Control: Operational List

Subject	Object	Operational list

Subject	Object	Operational list
A task to act for a user	***Document data***	***- Readout and print of the document data***

FDP_ACF.1 Access control by security attribute
FDP_ACF.1.1
The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].
[assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]: ***<Subject>*** ***- A task to act for a user*** ***<Subject attributes>*** ***- User identifier (User No.)*** ***----------*** ***<Object>*** ***- Document data*** ***<Object attributes>*** ***- Document data identifier***
[assignment: *access control SFP*]: ***Document data access control***
FDP_ACF.1.2
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]: ***<Operation control to document data>*** ***- A task to act for a user is permitted to read out and print out to the document data with the document data user identifier corresponding to the user identifier (user No.) of the subject attributes.***
FDP_ACF.1.3
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].
[assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]: ***None***
FDP_ACF.1.4
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].
[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]: ***None***
Hierarchical to : No other components Dependencies : FDP_ACC.1, FMT_MSA.3

6.1.1.3. Identification and Authentication

FIA_AFL.1	**Authentication failure handling**
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*].	
[assignment: *list of authentication events*]: ***Unsuccessful authentication to the administrator, CE, and the user***	
[selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]: ***[assignment: positive integer number]: 1***	
FIA_AFL.1.2	
When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].	
[assignment: *met, surpassed*]: ***Met***	
[assignment: *list of actions*]: ***Do not execute the next authentication attempt for 5 seconds to the administrator, CE and the user of unsuccessful authentication.***	
Hierarchical to :	No other components
Dependencies :	FIA_UAU.1 (FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3])

FIA_ATD.1	**User attribute definition**
FIA_ATD.1.1	
The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].	
[assignment: *list of security attributes*]: ***- User identifier (user No.)***	
Hierarchical to :	No other components
Dependencies :	No dependencies

FIA_SOS.1[1]	**Verification of secrets**
FIA_SOS.1.1[1]	
The TSF shall provide a mechanism to verify that secrets (***CE password***) meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*]: ***- Number of digits: 8-digits*** ***- Character type: Half size upper case alphabets, half size lower case alphabets, and half size numbers*** ***- Rules: Prohibit the same passwords as the passwords of previous generation.***	
Hierarchical to :	No other components
Dependencies :	No dependencies

FIA_SOS.1[2]	**Verification of secrets**
FIA_SOS.1.1[2]	
The TSF shall provide a mechanism to verify that secrets (***Administrator password***) meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*]: ***- Number of digits: 8-digits*** ***- Character type: Half size upper case alphabets, half size lower case alphabets, and half size numbers*** ***- Rules: Prohibit the same passwords as the passwords of previous generation.***	
Hierarchical to :	No other components
Dependencies :	No dependencies

FIA_SOS.1[3]	**Verification of secrets**
FIA_SOS.1.1[3]	
The TSF shall provide a mechanism to verify that secrets (***User password***) meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*]: ***- Number of digits: 8 to 64 digits*** ***- Character type: Half size upper case alphabets, half size lower case alphabets, and half size numbers*** ***- Rules: Prohibit the same passwords as the passwords of previous generation.***	
Hierarchical to :	No other components
Dependencies :	No dependencies

FIA_SOS.1[4]	**Verification of secrets**
FIA_SOS.1.1[4]	
The TSF shall provide a mechanism to verify that secrets (***HDD lock password***) meet [assignment: *a defined quality metric*].	
[assignment: *a defined quality metric*]: ***- Number of digits: 8 to 32 digits*** ***- Character type: Half size upper case alphabets, half size lower case alphabets, and half size numbers*** ***- Rules: None***	
Hierarchical to :	No other components
Dependencies :	No dependencies

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

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

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

FIA_UAU.7	**Protected authentication feedback**
FIA_UAU.7.1	
The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.	
[assignment: *list of feedback*]: ***Display "*" every character data input.***	
Hierarchical to :	No other components
Dependencies :	FIA_UAU.1 (FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3])

FIA_UID.2[1]	**User identification before any action**
FIA_UID.2.1[1]	
The TSF shall require each user (***CE***) to be successfully identified before allowing any other TSF-mediated actions on behalf of that user (***CE***).	
Hierarchical to :	FIA_UID.1
Dependencies :	No dependencies

FIA_UID.2[2]	**User identification before any action**
FIA_UID.2.1[2]	
The TSF shall require each user (***Administrator***) to be successfully identified before allowing any other TSF-mediated actions on behalf of that user (***Administrator***).	
Hierarchical to :	FIA_UID.1
Dependencies :	No dependencies

FIA_UID.2[3]	**User identification before any action**
FIA_UID.2.1[3]	
The TSF shall require each user (***user***) to be successfully identified before allowing any other TSF-mediated actions on behalf of that user (***user***).	
Hierarchical to :	FIA_UID.1
Dependencies :	No dependencies

FIA_USB.1	User-subject binding
FIA_USB.1.1	
The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].	
[assignment: *list of user security attributes*]: ***User identifier (user No.)***	
FIA_USB.1.2	
The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].	
[assignment: *rules for the initial association of attributes*]: **<For user identifier>** **- Associates the user No. of the relevant user to the task on the behalf of user when authenticated as the user.**	
FIA_USB.1.3	
The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].	
[assignment: *rules for the changing of attributes*]: ***None***	
Hierarchical to :	No other components
Dependencies :	FIA_ATD.1

6.1.1.4. Security Management

FMT_MOF.1	Management of security functions behavior
FMT_MOF.1.1	
The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].	
[assignment: *list of functions*]: ***- Enhanced Security Mode***	
[selection: *determine the behavior of, disable, enable, modify the behavior of*] : ***disable***	
[assignment: *the authorized identified roles*]: ***Administrator***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1, FMT_SMR.1 (FMT_SMR.1[2])

FMT_MSA.3	Static attribute initialization
FMT_MSA.3.1	
The TSF shall enforce the [*assignment: access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes (***document data user identifier***) that are used to enforce the SFP.	
[selection, choose one of: *restrictive, permissive, [assignment: other property]*] [assignment: *other property*]: ***User No.***	
[assignment: *access control SFP, information flow control SFP*] ***Document data access control***	
Refinement: “Security attribute” -> “Document data user identifier”	
FMT_MSA.3.2	
The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.	

[assignment: *the authorized identified roles*] ***None***		
Hierarchical to	:	No other components
Dependencies	:	FMT_MSA.1 (N/A), FMT_SMR.1(N/A)

FMT_MTD.1[1]	**Management of TSF data**
FMT_MTD.1.1[1]	
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].	
[assignment: *list of TSF data*]: ***- User No.*** ***- User password***	
[selection: *change_default, query, modify, delete*, clear, [assignment: *other operations*]]: ***[assignment: other operations]: Registration***	
[assignment: *the authorized identified roles*]: ***Administrator***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1, FMT_SMR.1 (FMT_SMR.1[2])

FMT_MTD.1[2]	**Management of TSF data**
FMT_MTD.1.1[2]	
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].	
[assignment: *list of TSF data*]: ***User password***	
[selection: *change_default, query, modify, delete*, clear, [assignment: *other operations*]]: ***Modify***	
[assignment: *the authorized identified roles*]: ***- User*** ***- Administrator***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1, FMT_SMR.1 (FMT_SMR.1[2], FMT_SMR.1[3])

FMT_MTD.1[3]	**Management of TSF data**
FMT_MTD.1.1[3]	
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].	
[assignment: *list of TSF data*]: ***Administrator password***	
[selection: *change_default, query, modify, delete*, clear, [assignment: *other operations*]]: ***Modify***	
[assignment: *the authorized identified roles*] : ***- Administrator*** ***- CE***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1, FMT_SMR.1 (FMT_SMR.1[1], FMT_SMR.1[2])

FMT_MTD.1[4]	**Management of TSF data**
FMT_MTD.1.1[4]	
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].	
[assignment: *list of TSF data*]: ***CE password***	
[selection: *change_default, query, modify, delete*, clear, [assignment: *other operations*]]: ***Modify***	
[assignment: *the authorized identified roles*]: ***CE***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1, FMT_SMR.1 (FMT_SMR.1[1])

FMT_MTD.1[5]	**Management of TSF data**
FMT_MTD.1.1[5]	
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].	
[assignment: *list of TSF data*]: ***- Administrator password*** ***- CE password***	
[selection: *change_default, query, modify, delete*, clear, [assignment: *other operations*]]: ***[assignment: other operations]: Registration***	
[assignment: *the authorized identified roles*]: ***CE***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1, FMT_SMR.1 (FMT_SMR.1[1])

FMT_MTD.1[6]	**Management of TSF data**
FMT_MTD.1.1[6]	
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].	
[assignment: *list of TSF data*]: ***HDD lookout password***	
[selection: *change_default, query, modify, delete*, clear, [assignment: *other operations*]]: ***Modify***	
[assignment: *the authorized identified roles*]: ***Administrator***	
Hierarchical to :	No other components
Dependencies :	FMT_SMF.1, FMT_SMR.1 (FMT_SMR.1[2])

FMT_MTD.1[7]	**Management of TSF data**
FMT_MTD.1.1[7]	
The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].	
[assignment: *list of TSF data*]: ***User No.***	
[selection: *change_default, query, modify, delete*, clear, [assignment: *other operations*]]: ***Delete***	

[assignment: *the authorized identified roles*]: ***Administrator***		
Hierarchical to	:	No other components
Dependencies	:	FMT_SMF.1, FMT_SMR.1 (FMT_SMR.1[2])

FMT_SMF.1	**Specification of Management Functions**
FMT_SMF.1.1	
The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF*].	
[assignment: *list of management functions to be provided by the TSF*]: ***- Stop Function of Enhanced security mode by administrator*** ***- Registration function of user No. by administrator*** ***- Deletion function of user No. by administrator*** ***- Registration function of user password by administrator*** ***- Modification function of user password by administrator*** ***- Modification function of HDD lock password by administrator*** ***- Modification function of user password by user*** ***- Modification function of administrator password by administrator*** ***- Registration function of CE password by CE*** ***- Modification function of CE password by CE*** ***- Registration function of administrator password by CE*** ***- Modification function of administrator password by CE***	
Hierarchical to	: No other components
Dependencies	: No dependencies

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

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

FMT_SMR.1[3]	**Security roles**
FMT_SMR.1.1[3]	

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

6.1.1.5. Protection of TSF

FPT_STM.1	**High-reliable time stamp**
FPT_STM.1.1	
The TSF shall be able to provide reliable time stamps.	
Hierarchical to :	No other components
Dependencies :	No dependencies

FPT_TEE.1	**External entity test**
FPT_TEE.1.1	
The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*] to check the fulfillment of [assignment: *list of properties of the external entities*] .	
[assignment: *list of properties of the external entities*] ***Authentication by the HDD lock password shall be successful on the external entity (HDD) connected to TOE.***	
[selection: *during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*]] ***during initial startup***	
FPT_TEE.1.2	
If the test fails, the TSF shall [assignment: *action(s)*] .	
[assignment: *action(s)*] ***Stop the operation of TOE and MFP main body.***	
Hierarchical to :	No other components
Dependencies :	No dependencies

6.1.2. TOE Security Assurance Requirements

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

Table 5 TOE Security Assurance Requirements

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

6.2. IT Security Requirements Rationale

6.2.1. Rationale for IT Security Functional Requirements

6.2.1.1. Necessity

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

Table 6 Conformity of IT Security Functional Requirements to Security Objectives

Security Objectives / Security Functional Requirements	O.IA	O.ACCESS	O.MANAGE	O.AUDIT	O.CHECK-HDD
FAU_GEN.1				●	
FAU_STG.1				●	
FAU_STG.4				●	
FAU_SAR.1				●	
FAU_SAR.2				●	
FDP_ACC.1		●			
FDP_ACF.1		●			
FIA_AFL.1	●				
FIA_ATD.1		●			
FIA_SOS.1[1]			●		
FIA_SOS.1[2]			●		
FIA_SOS.1[3]	●		●		
FIA_SOS.1[4]			●		
FIA_UAU.2[1]	●				
FIA_UAU.2[2]	●				
FIA_UAU.2[3]	●				
FIA_UAU.7	●				
FIA_UID.2[1]	●				
FIA_UID.2[2]	●				
FIA_UID.2[3]	●				
FIA_USB.1		●			
FMT_MOF.1	●	●	●	●	
FMT_MSA.3		●			
FMT_MTD.1[1]			●		
FMT_MTD.1[2]	●		●		
FMT_MTD.1[3]			●		
FMT_MTD.1[4]			●		
FMT_MTD.1[5]			●		
FMT_MTD.1[6]			●		
FMT_MTD.1[7]			●		
FMT_SMF.1	●	●	●		
FMT_SMR.1[1]			●		
FMT_SMR.1[2]			●		
FMT_SMR.1[3]	●	●			
FPT_STM.1				●	
FPT_TEE.1					●

6.2.1.2. Sufficiency

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

- **O.IA (Identification and authentication at use)**
  This security objective requires the functions for identification and authentication for the user, CE, and the administrator, and needs various requirements regarding identification and authentication are required.

It can be ensured that operations are performed by a valid CE by identifying that a person who intends to access is a registered CE with FIA_UID.2[1] and authenticating the person with FIA_UAU.2[1]. It can be ensured that operations are performed by a valid administrator by identifying that a person who intends to access is a registered administrator with FIA_UID.2[2] and authenticating the person with FIA_UAU.2[2]. Also it is ensured that operations is performed by a valid user by identifying that a person who intends to access is a registered user with FIA_UID.2[3] and authenticating the user with FIA_UAU.2[3].
When authentication for the administrator, CE, or user fails, FIA_AFL.1 makes the administrator, CE, or user wait for 5 seconds until the next authentication attempt to prolong the length of duration for an invalid user succeeds the authentication as the administrator, CE, and user. Additionally FIA_UAU.7 displays dummy characters (*) equivalent to the number of characters input in the password input field to keep the password secret.
FMT_MTD.1[2] permits the identified and authenticated user who owns the document data to modify the relevant user password. Modification of password reduces the possibility that a user password input by an illegal user matches with the valid password.
The user password is verified whether it conforms to the password rule specified by FIA_SOS.1[3] when the user password is modified. FMT_SMF.1 identifies the password management. FMT_SMR.1[3] maintains the target users. The above function operates actively with FMT_MOF.1. Therefore, the security objective O.IA is feasible with the relevant security functional requirements (FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.7, FIA_UID.2[1], FIA_UID.2[2], FIA_UID.2[3], FIA_AFL.1, FMT_MTD.1[2], FIA_SOS.1[3], FMT_SMF.1, FMT_SMR.1[3], and FMT_MOF.1).

- **O.ACCESS (Access control for document data)**
  This security objective limits the access to document data to the user who owns the relevant document data, and needs various requirements that relate to the access control.

  A value of security attribute of document data (document data identifier) that a user, registered by the administrator in advance with FMT_MSA.3, generates is set to a value of the user identifier (user No.) registered by the administrator. When a user identifier is associated with the task, which acts for a user by FIA_ATD.1, and FIA_USB.1, the access control is implemented with FIA_ACC.1, and FDP_ACF.1. Moreover, when O.ACCESS permits the function that enables for a valid user who owns the document data to read out the document data, only the valid user who owns the document data can refer to the document data.
  Each object user is also maintained with FMT_SMR.1[3], and the management for user identifier is identified with FMT_SMF.1. The above function operates actively with FMT_MOF.1.

  Therefore, O.ACCESS is feasible with the relevant security functional requirements (FIA_ATD.1, FIA_USB.1, FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_SMR.1[3], FMT_SMF.1, and FMT_MOF.1).

- **O.MANAGE (Provision of management function)**
  This security objective limits the functions related to settings of the enhanced security mode to the administrator, and needs various requirements to limit the access to a series of setting function and the management function.

  CE can register the administrator password with FMT_MTD.1[5]. The administrator is registered in

TOE by registration of the administrator password, and is enabled to start the operations as the administrator. Since CE can register the own password of CE with FMT_MTD.1[5] and modify it with FMT_MTD.1[4], CE can modify the passwords of CE and administrator every appropriate interval. In addition, since it is verified that the CE and administrator passwords conform to the password rule specified by FIA_SOS.1[1] and FIA_SOS.1[2] when the password is modified, it reduces the possibility that the password of CE or administrator input by a user matches with the valid password of CE or administrator.

FMT_SMF.1 identifies the management for CE password and administrator password. FMT_SMR.1[1] and FMT_SMR.1[2] maintain the administrators and CE. The above function operates actively with FMT_MOF.1.

FMT_MTD.1[1] permits the registration function of user No. and user password to only the administrator, and FMT_MTD.1[2] permits the modification function of user password to only the user and administrators. The user password is verified whether it conforms to the password rule specified by FIA_SOS.1[3] when the user password is registered. Additionally FMT_MTD.1[7] permits the deletion function of the user No. only to the administrator.

FMT_MTD.1[6] provides the function to the administrator that enables modification and management of the lock passwords of HDD1-6. These passwords are verified whether those conform to the rule specified by FIA_SOS.1[4].

Since FMT_MTD.1[3] permits the administrator to modify own password, the administrator is enabled to modify the administrator password every appropriate interval. The administrator password is verified whether it conforms to the password rule specified by FIA_SOS.1[2] when the administrator password is modified.

FMT_SMF.1 identifies the password management of user No. and user password. FMT_SMR.1[2] maintains the administrators. FMT_MOF.1 permits only the administrator to stop the enhanced security mode.

Therefore, O.MANAGE is feasible with the relevant security functional requirements (FMT_MTD.1[2], FMT_MTD.1[4], FMT_MTD.1[5], FMT_MTD.1[7], FIA_SOS.1[1], FIA_SOS.1[2], FMT_SMR.1[1], FMT_MTD.1[1], FIA_SOS.1[3], FIA_SOS.1[4], FMT_MTD.1[3], FIA_SOS.1[2], FMT_SMF.1, FMT_SMR.1[2], and FMT_MOF.1).

- **O.AUDIT (Audit evidence)**

This security objective needs the function to generate the audit log, the function to limit the reference to the audit log, and the various requirements related to prevention of loss of the audit data.

FPT_STM.1 records the necessary audit information together with the reliable time stamps with FAU_GEN.1. Since the operation logs such as unsuccessful identification and authentication of user, registration/deletion of user No., registration/modification of user passwords, readout and print of document data as all the events relevant to explicit irregular accesses to the "assets of protection objects" are recorded as the audit logs, the administrator can detect irregular accesses to the document data by referring to these audit logs. In addition, the successful operations to the TSF data such as registration/modification of the CE and administrator password are recorded in the audit logs, the administrator can detect the impersonation to CE and administrator through referring the audit logs by the administrator. Furthermore, detection of the attempts to modify the HDD password and use the relevant management function irregularly by a person who impersonates to the administrator because O.AUDIT records the unsuccessful administrator identification-authentication events, successful enhanced security mode setting events, and

successful HDD lock password modification events as the audit information.
FAU_STG.1 protects the audit storage area, and FAU_STG.4 overwrites the audit logs in the old audit log area if the prepared audit storage area is exhausted. The audit information collection operates actively with FMT_MOF.1. Thus, the necessary audit information is stored. Furthermore, FAU_SAR.2 prohibits the readout of audit logs by other than the administrator and CE. FAU_SAR.1 provides the audit logs as various interpretable formats. Thus, the audit for the audit logs is possible.
Therefore, O.AUDIT is feasible with the relevant security functional requirements (FPT_STM.1, FAU_GEN.1, FAU_STG.1, FAU_STG.4, FMT_MOF.1, FAU_SAR.2, and FAU_SAR.1).

- **O.CHECK-HDD (Verification of HDD)**
  This security objective needs the HDD lock function using the HDD lock passwords set to check that the HDD to which the HDD lock password is set before TOE is started up, and various requirements that specify the operation test for external entities.
  FPT_TEE.1 delivers the HDD lock password to the HDD at startup of TOE, and, stops the operation of TOE and MFP main body if authentication by the HDD lock password fails for the relevant HDD.
  Therefore, the O.HDD-LOCK is feasible with the relevant security functional requirement (FPT_TEE.1).

6.2.1.3. Dependencies of IT Security Functional Requirements

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

Table 7 Dependencies of IT Security Functional Requirements Components

N/A: Not Applicable

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3]
FIA_ATD.1	None	N/A
FIA_SOS.1[1]	None	N/A
FIA_SOS.1[2]	None	N/A
FIA_SOS.1[3]	None	N/A
FIA_SOS.1[4]	None	N/A
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1]
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2]
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3]
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3]
FIA_UID.2[1]	None	N/A

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FIA_UID.2[2]	None	N/A
FIA_UID.2[3]	None	N/A
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	N/A (Since the security attribute of subject (user) and object (document data) is always fixed land reference is also disabled. this relationship is unnecessary. And assignment of FMT_MSA.3.2 is N/A. FMT_SMR.1 is the dependency set related to the left column, application is unnecessary.)
FMT_MTD.1[1]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2]
FMT_MTD.1[2]	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2], FMT_SMR.1[3]
FMT_MTD.1[3]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1], FMT_SMR.1[2]
FMT_MTD.1[4]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]
FMT_MTD.1[5]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[1]
FMT_MTD.1[6]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_MTD.1[7]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1[2]
FMT_SMF.1	None	N/A
FMT_SMR.1[1]	FIA_UID.1	FIA_UID.2[1]
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[2]
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[3]
FPT_STM.1	None	N/A
FPT_TEE.1	None	N/A

6.2.2. Rationale for IT Security Assurance Requirements

This TOE is installed and used in an environment where adequate security is maintained in terms of the physical, personnel, and connectivity. Nonetheless, adequate effectiveness in the environment where TOE is used must be assured. As a general commercial office product, the execution of tests based on function specifications and TOE design, and analysis of the strength of function and a search for vulnerabilities are required. In addition, it is desirable that it has a development environment control, a configuration management for TOE and a secure distribution procedure. And therefore the selection of EAL3, which provides an adequate assurance level, is reasonable.
The secure requirement dependency analysis is assumed to be appropriate because the package EAL has been selected, therefore details are not discussed.

7. TOE Summary Specification

In this chapter, TOE summary specification is described.

7.1. TOE Summary Specification

In this section, TOE security functions are described. As TOE security functional requirements corresponding to respective functions are shown, the security function described in this section satisfies TOE security functional requirements described in 6.1.1.

7.1.1. Identification and Authentication

The identification and authentication function has the following security function groups.

Function Name	Security Function Specifications	TOE Security Functional Requirements
IA.ADM_ADD Registration of administrator Registration of CE	IA.ADM_ADD registers the CE and administrators in TOE. Only the CE operates IA.ADM_ADD. The CE registers the passwords of CE and administrators. IA.ADM_ADD provides the interface for registration of CE and administrators. The interface for registration of CE and administrators requires input of the password relevant to each CE and administrator. The allowable values are verified for the passwords for CE and administrators input by the CE according to the following rules. - Password shall consist of eight characters. - Password shall consist of half size upper case alphabets, half size lower case alphabets, and half size numbers. - Use of the same password values as the password values of previous generation is prohibited. In the verification of allowable values, if the rules are complied, the CE and administrators are registered. If the rules are not complied, registration is rejected.	FIA_SOS.1[1] FIA_SOS.1[2] FMT_MTD.1[5] FMT_SMF.1 FMT_SMR.1[1]
IA.ADM_AUTH Identification and authentication of administrator	IA.ADM_AUTH identifies an operator is the administrator registered in TOE before the operator uses TOE, and authenticates personal identification of the administrator. IA.ADM_AUTH does not permit any operations of the management functions before identification and authentication of the administrator. The interface for identification and authentication of the administrator requires registration with IA.ADM_ADD and input of a modified password with IA_PASS. IA.ADM_AUTH identifies the administrator from the indication of the interface for identification and authentication of administrator, and authenticates personal identification of the administrator based on the input password. When the administrator inputs the password, it displays the dummy characters (*) instead of the input password. When authentication fails, it provides the interface for	FIA_AFL.1 FIA_UAU.2[2] FIA_UAU.7 FIA_UID.2[2]

	identification and authentication of the administrator after five seconds.	
IA.CE_AUTH Identification and authentication of CE	IA.CE_AUTH identifies an operator is the CE registered in TOE before the operator uses TOE, and authenticates personal identification of the CE. IA.CE_AUTH does not permit any operations of the CE functions before identification and authentication of the CE. It requires the password modified with IA_PASS. IA.CE_AUTH identifies the CE from the indication of the interface for identification and authentication of CE, and authenticates personal identification of the CE based on the input password. When the CE inputs the password, it displays the dummy characters (*) instead of the input password. When authentication fails, it provides the interface for identification and authentication of the CE after five seconds.	FIA_AFL.1 FIA_UAU.2[1] FIA_UAU.7 FIA_UID.2[1]
IA.PASS Modification of password	IA.PASS modifies the administrator password, CE password, and user password that are the authentication information for the administrator, CE, and user. IA.PASS provides the interface for password modification, and requires input of a new password. Each user can modify the following passwords. CE: CE password and administrator password Administrator: Administrator password and user password User : Own user box password The allowable values are verified for the passwords input by CE, administrators and user according to the following rules. - The CE and administrator passwords shall consist of eight characteristics. - The user password shall consist of 8 to 64 characters. - Password shall consist of half size upper case alphabets, half size lower case alphabets, and half size numbers. - Use of the same password values as the password values of previous generation is prohibited. In the verification of allowable values, if the rules are complied, the password is modified.	FIA_SOS.1[1] FIA_SOS.1[2] FIA_SOS.1[3] FMT_MTD.1[2] FMT_MTD.1[3] FMT_MTD.1[4] FMT_SMF.1 FMT_SMR.1[1] FMT_SMR.1[2] FMT_SMR.1[3]

7.1.1.1. Method to Realize Relevant SFR

FIA_AFL.1

This not executes the following authentication attempts for five seconds to the administrator with IA.ADM_AUTH and the CE with IA.CE_AUTH.

FIA_SOS.1[1]

This judges whether the password value is within the allowable range according to the password rules for CE password registration with IA.ADM_ADD and CE password modification with IA.PASS. As described above, FIA_SOS.1[1] can be realized by implementation of IA.PASS.

FIA_SOS.1[2]

This judges whether the password value is within the allowable range according to the password rules for administrator password registration with IA.ADM_ADD and administrator and CE passwords modification with IA.PASS.

As described above, FIA_SOS.1[2] can be realized by implementation of IA.ADM_ADD and IA.PASS.

FIA_SOS.1[3]

This judges whether the value is within the range of allowable value according to the password rules for user password modification with IA.PASS. As described above, FIA_SOS.1[3] can be realized by implementation of IA.PASS.

FIA_UAU.2[1]

This authenticates the CE with IA.CE_AUTH. As described above, FIA_UAU.2[1] can be realized by implementation of IA.CE_AUTH.

FIA_UAU.2[2]

This authenticates the administrator with IA.ADM_AUTH. As described above, FIA_UAU.2[2] can be realized by implementation of IA.ADM_AUTH.

FIA_UAU.7

This displays the input password by the dummy characters (*) equal to the number of input characters at password input for authentication of the administrator with IA.ADM_AUTH and for authentication of the CE with IA.CE_AUTH. As described above, FIA_UAU.7 can be realized by implementation of IA.ADM_AUTH and IA.CE_AUTH.

FIA_UID.2[1]

This identifies the CE with IA.CE_AUTH. As described above, FIA_UID.2[1] can be realized by implementation of IA.CE_AUTH.

FIA_UID.2[2]

This identifies the administrator with IA.ADM_AUTH. As described above, FIA_UID.2[2] can be realized by implementation of IA.ADM_AUTH.

FMT_MTD.1[2]

This permits modification of the user password to the administrator and user with IA.PASS, and executes modification. As described above, FMT_MTD.1[2] can be realized by implementation of IA.PASS.

FMT_MTD.1[3]

This permits and executes the administrator and CE to modify the administrator password with IA.PASS. As described above, FMT_MTD.1[3] can be realized by implementation of IA.PASS.

FMT_MTD.1[4]

This permits and executes only the CE to modify the CE password with IA.PASS. As described above, FMT_MTD.1[4] can be realized by implementation of IA.PASS.

FMT_MTD.1[5]

This permits and executes only the CE to register the CE and administrator passwords with IA.ADM_ADD. As described above, FMT_MTD.1[5] can be realized by implementation of IA.ADM_ADD.

FMT_SMF.1

This implements the function that manages the CE and administrator passwords with IA.ADM_ADD. This implements the function that manages the administrator, CE, and user passwords with IA.PASS. As described above, FMT_SMF.1 can be realized by implementation of IA.ADM_ADD and IA.PASS.

FMT_SMR.1[1]

The roll of CE is maintained by managing the CE password. Therefore, maintenance of this roll is realized by limiting the operation of CE password modification only to the CE. This limitation is implemented with IA.PASS. As described above, FMT_SMR.1[1] can be realized by implementation of IA.PASS.

FMT_SMR.1[2]

The roll of administrator is maintained by managing the administrator password. Therefore, maintenance of this roll is realized by limiting the operation of administrator password modification only to the CE and administrators. This limitation is implemented with IA.PASS. As described above, FMT_SMR.1[2] can be realized by implementation of IA.PASS.

FMT_SMR.1[3]

The roll of user is maintained by managing the relevant user password. Therefore, maintenance of this roll is realized by limiting the operation of user password modification only to the administrators and user. This limitation is implemented with IA.PASS.
As described above, FMT_SMR.1[3] can be realized by implementation of IA.PASS.

7.1.2. Access Control

The access control function has the following security function groups.

Function Name	Security Function Specifications	TOE Security Functional Requirements
ACL.USR Access rules and control for user	ACL.USR identifies and authenticates the user. When this can authenticate personal identification of the user, this limits the operation range available for the user according to the access control rules. ACL.USR identifies and authenticates the user based on the user identifier and the user password. This displays the dummy characters (*) instead of the input password when the user inputs the user password. After identification and authentication is completed successfully, this permits the following operations to the document data indicated by the user identifier that has been identified and authenticated. - Readout and print of the document data After identification and authentication is completed successfully, the contents of the document data associated with the relevant user identifier are displayed on the panel, and print are permitted only to the displayed document (other	FDP_ACC.1 FDP_ACF.1 FIA_AFL.1 FIA_ATD.1 FIA_UAU.2[3] FIA_UAU.7 FIA_UID.2[3] FIA_USB.1 FMT_MSA.3

	document data owned by the other users is not displayed). If identification and authentication result in failure, the interface for identification and authentication shall be made active after five seconds.	

7.1.2.1. Method to Realize Relevant SFR

FDP_ACC.1

ACL.USR limits readout and print of the document data only to the user according to the document data access control. As described above, FDP_ACC.1 can be realized by implementation of ACL.USR.

FDP_ACF.1

ACL.USR limits readout and print of the document data only to the user according to the document data access control. As described above, FDP_ACF.1 can be realized by implementation of ACL.USR.

FIA_AFL.1

If user authentication fails, the next authentication attempt is not executed for 5 seconds to the user. As described above, FIA_AFL.1 can be realized by implementation of ACL.USR.

FIA_ATD.1

After successful completion of identification and authentication of user, the user identifier is associated with the task on behalf of the relevant user. As described above, FIA_ATD.1 can be realized by implementation of ACL.USR.

FIA_UAU.2[3]

ACL.USR executes user authentication. As described above, FIA_UAU.2[3] can be realized by implementation of ACL.USR.

FIA_UAU.7

ACL.USR displays the input password by the dummy characters (*) equal to the number of input characters at user password input for authentication. As described above, FIA_UAU.7 can be realized by implementation of ACL.USR.

FIA_UID.2[3]

ACL.USR executes user identification. As described above, FIA_UID.2[3] can be realized by implementation of ACL.USR.

FIA_USB.1

After successful completion of identification and authentication of the user, the user identifier is associated with the task on behalf of the relevant user. As described above, FIA_USB.1 can be realized by implementation of ACL.USR.

FMT_MSA.3

ACL.USR sets the user identifier value to the default value of the document data user identifier that is the security attribute of the document data when the user creates the document data. As

described above, FMT_MSA.3 can be realized by implementation of ACL.USR.

7.1.3. Audit

The audit function has the following security function groups.

Function Name	Security Function Specifications	TOE Security Functional Requirements
AUD.LOG Audit information log	AUD.LOG records the audit information on the security function as the list of correct date and time (YY:MM:DD:hh:mm:ss), identification information of the operation actors, and information of the event results. The following events are the audit targets. - Activation and termination of the audit function - Success and failure in identification and authentication of the administrator, CE, and user - Success in registration of the CE password - Success in registration of the administrator password, user No. and user password - Success in modification of the administrator, CE, and user password - Success in readout and print of the document data - Success in print of the audit log - Success in output of the audit log to USB - Success in settings of the enhanced security mode - Success in deletion of the user (user No.) by the administrator - Success in modification of the HDD lock password	FAU_GEN.1 FPT_STM.1
AUD.MNG Management of audit area	AUD.MNG manages the audit storage area to create and store the audit information. The area to store the audit information shall be the memory area of ring buffer type. AUD.MNG overwrites the audit information from the top of memory area when the audit information storage area is exhausted.	FAU_STG.4

7.1.3.1. Method to Realize Relevant SFR

FAU_GEN.1

As the audit information of security function operations, AUD.LOG records startup/stop of the audit function, success/failure of identification and authentication, success in registration of the CE, administrator, and user, success in modification of the administrator password, CE password, user password, and HDD lock password, success in readout and print of the document data, success in print and output of the audit log to USB, and success in the settings of enhanced security mode, and deletion of the user, in combination with correct date and time (YY:MM:DD:hh:mm:ss) and the identification information of operation actors. As described above, FAU_GEN.1 can be realized by implementation of AUD.LOG.

FAU_STG.4

When the audit storage area is exhausted, AUD.MNG overwrites the audit information in the old storage area. As described above, FAU_STG.4 can be realized by implementation of AUD.MNG.

FPT_STM.1

AUD.LOG realizes the function that crease the necessary audit information in combination with the reliable time stamps. Thus, FPT_STM.1 can be realized by implementation of AUD.LOG.

7.1.4. Management Assistance

The management assistance function has the following security function groups.

Function Name	Security Function Specifications	TOE Security Functional Requirements
MNG.MODE Settings of enhanced security mode	MNG.MODE permits the function to stop the enhanced security mode only to the administrator and executes this function.	FMT_MOF.1 FMT_SMF.1
MNG.ADM Management Assistance function (Administrator)	MNG.ADM permits the following processing to the administrator and executes the processing. (Query of the audit information is permitted also to CE.) - Registration of the user identifier and user password - Deletion of the user (deletion of the user No.) - Query of the audit information (the function to delete the audit information is not provided.) Verification of the allowable value for the user password input by the administrator according to the following rules - The password shall consist of 8 to 64 characters. - The password shall consist of half size upper case alphabets, half size lower case alphabets, and half size numbers. - Use of the same password values as the password values of previous generation is prohibited. In the verification of allowable values, if the rules are complied, the password is registered. If the rules are not complied, registration is rejected. The query result of audit information is printed or output to USB in the format that can be referred by the administrator and CE only, where includes the information of date and time when events occurred (YY:MM:DD:hh:mm:ss), identification information of the operation actors, and information of the event results.	FAU_SAR.1 FAU_SAR.2 FAU_STG.1 FIA_SOS.1[3] FMT_MTD.1[1] FMT_MTD.1[7] FMT_SMF.1 FMT_SMR.1[2]
MNG.HDD HDD lookout password function	MNG.HDD permits the following processing to the administrator only and executes the processing. - Modification of the HDD lock password The allowable values are verified for the HDD lock passwords input by the administrator according to the following rules.	FIA_SOS.1[4] FMT_MTD.1[6] FMT_SMF.1 FMT_SMR.1[2]

	- The password shall consist of 8 to 32 characters. - The password shall consist of half size upper case alphabets, half size lower case alphabets, and half size numbers. In the verification of allowable values, if the rules are complied, the HDD lock password set to the HDD device is modified. If the rules are not complied, modification is rejected.	

7.1.4.1. Method to Realize Relevant SFR

FAU_SAR.1

MNG_ADM enables for the administrator and CE to refer to the audit records. As described above, FAU_SAR.1 can be realized by implementation of MNG_ADM.

FAU_SAR.2

The interface for access to the audit records exists only in the administrator mode (accessible only after successful identification and authentication of the administrator) and the service mode (accessible only after successful identification and authentication of the CE). MNG.ADM limits the access so that only the administrator and CE can refer to the audit records. As described above, FAU_SAR.2 can be realized by implementation of MNG.ADM.

FAU_STG.1

MNG.ADM implements the function that allows only the administrator and CE to read out and print the data within the audit storage area. It does not provide the function that allows deletion and modification of the data within the audit storage area. As described above, FAU_STG.1 can be realized by implementation of MNG.ADM.

FIA_SOS.1[3]

For registration/modification of the user password, MNG_ADM judges whether the password value is within the range of allowable value according to the password rules. As described above, FIA_SOS.1[3] can be realized by implementation of MNG_ADM.

FIA_SOS.1[4]

For modification of the HDD lock password, MNG_HDD judges whether the password value is within the range of allowable value according to the password rules. As described above, FIA_SOS.1[4] can be realized by implementation of MNG_HDD.

FMT_MOF.1

MNG.MODE permits the function to stop the enhanced security mode of TOE only to the administrator and execute it. As described above, FMT_MOF.1 can be realized by implementation of MNG.MODE.

FMT_MTD.1[1]

MNG.ADM permits registration of the user No. and user password only to the administrator and execute it. As described above, FMT_MTD.1[1] can be realized by implementation of MNG.ADM.

FMT_MTD.1[6]

MNG_HDD realizes the function to input the HDD lock password. As described above,

FMT_MTD.1[6] can be realized by implementation of MNG_HDD.

FMT_MTD.1[7]

MNG.ADM permits the administrator to delete the user No. and executes deletion. As described above, FMT_MTD.1[7] can be realized by implementation of MNG.ADM.

FMT_SMF.1

MNG.MODE implements the function to stop the enhanced security mode, MNG.ADM implements the function to manage the user by registration/deletion of the user identifier and registration of the user password, and MNG.HDD implements the function to modify the HDD lock password. As described above, FMT_SMF.1 can be realized by implementation of MNG.MODE, MNG.ADM, and MNG.HDD.

FMT_SMR.1[2]

This is the function that maintains the roll as administrator and is related to FMT_MTD.1[6] and FMT_MTD.1[7]. This function can be realized by IA.PASS.

7.1.5. Test function of HDD lock system

Test function of HDD lock system has the following security function group.

Function Name	Security Function Specifications	TOE Security Functional Requirements
HDD-LOCK. TEST Test of HDD lock function	HDD-LOCK. TEST is the function provided to enable TOE to implement the test of HDD lock function to the HDDs that are connected to TOE. At startup of TOE, TOE checks the status of each HDD (HDD1-6) for locked/unlocked, and, if it is confirmed all the HDDs are in the locked status, TOE requests the unlock processing by the HDD lock passwords (if it is confirmed that either HDD is in the unlocked status, TOE stops the operation by the error processing). In the unlock processing by the HDD lock password, TOE sends the HDD lock passwords to all the HDDs, and TOE activates the HDDs only when the HDD passwords authentication successes in all the HDDs. If failure of the unlock processing by the HDD lock password is confirmed in either HDD, TOE stops the operation of TOE and the MFP main body.	FPT_TEE.1

7.1.5.1. Method to Realize Relevant SFR

FPT_TEE.1

FPT_TEE.1 can be realized because the predefined HDD lock passwords are delivered to the HDDs at startup of the MFP, the unlock operation is requested which unlocks the HDD locked status set by the HDD lock function of the HDD, and TOE and the MFP main body operation are stopped if the authentication by the HDD lock password fails.

---END---