4036 Multi-Function Peripheral Control Software Security Target

This document is a translation of the security target written in Japanese, which has been evaluated and certified. The Japan Certification Body has reviewed and checked it.

Version: 1.07

Issued on: August 5, 2004

Created by: KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

<Revision history>

Date	Ver.	Approved	Checked	Created	Revision
02/27/2004	1.00	Hirota	Goto	Nakayama	Initial version.
03/30/2004	1.01	Hirota	Goto	Nakayama	Typos corrected.
04/02/2004	1.02	Hirota	Goto	Nakayama	Corrections.
04/14/2004	1.03	Hirota	Goto	Nakayama	Corrections for the Observation Report (ASE001-01 to ASE007-01).
05/14/2004	1.04	Hirota	Goto	Nakayama	Corrections for the Observation Report (ASE008-01 to ASE013-01).
06/25/2004	1.05	Hirota	Goto	Nakayama	Corrections for the Observation Report (ASE014-01 to ASE017-01).
08/03/2004	1.06	Hirota	Goto	Nakayama	Corrections for the Observation Report (ASE018-01 to ASE019-01).
08/05/2004	1.07	Hirota	Goto	Nakayama	Corrections for the Observation Report (ASE020-01).

Table of Contents

---- *(Figure List)* ---

---- *(Table List)* ---

1. ST Introduction

1.1. ST Identification

- ST Title: #4036 Multi-Function Peripheral[1], Control Software

  Security Target
- Version: 1.07
- CC version: 2.1
- Created on: August 5, 2004
- Created by: KONICA MINOLTA BUSINESS TECHNOLOGIES, INC.

1.2. TOE Identification

- TOE Name: Japan: #4036 Multi-Function Peripheral Zentai Seigyo Software

  Overseas: #4036 Multi-Function Peripheral Control Software
- TOE Version: * TOE is comprised of the following two software components, "Macro System Controller" and "Network Module." Each has its own version.
  - ➢ User Interface: 4036-10G0-18-00
  - ➢ Network Module: 4036-A0G0-04-00
- TOE type: Software
- Created by: KONICA MINOLTA BUSINESS TECHONOLOGIES, INC.

1.3. CC Conformance Claim

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

- Security function requirement

[1] "#4036 Multi-Function Peripheral" is a multi-function peripheral offered to consumers under the commercial names "bizhub C350," "CF2203," and "8022."

CC Version 2.1, Part2 Conformant

- Security assurance requirement

  CC Version 2.1, Part3 Conformant

- Evaluation assurance level

  EAL3 Conformant (No additional assurance component)

- PP Reference

  This ST does not carry out a PP reference.

- **References**

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model Version 2.1 August 1999 CIMB-99-031

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements Version 2.1 August 1999 CCIMB-99-032

- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements Version 2.1 August 1999 CCIMB-99-033

- CCIMB Interpretations - 0210

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model Version 2.1 August 1999 CIMB-99-031 (January 2001 Translation Version 1.2, Information-technology Promotion Agency Japan, Security Center)

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements Version 2.1 August 1999 CCIMB-99-032 (January 2001 Translation Version 1.2, Information-technology Promotion Agency Japan, Security Center)

- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements Version 2.1 August 1999 CCIMB-99-033 (January 2001 Translation Version 1.2, Information-technology Promotion Agency Japan, Security Center)

- CCIMB Interpretations – 0210 (Translation Version)

1.4. ST Overview

#4036 Multi-Function Peripheral (hereafter, “MFP”) is Konica Minolta Business Technologies, Inc. digital MFP comprised by selecting and combining copy, print and scan functions. The target of evaluation (TOE) of this Security Target (ST) is the “#4036 Multi-Function Peripheral Control Software,” that is comprised of “Macro System Controller,” which is a software component that carries out operational control processes from MFP operation panel, job resources management, and job sequence control processes and “Network Module,” which is a software component that carries out operational control processes from the client PC, from among the built-in control software in #4036 MFP. This ST explains the security functions that are realized by the TOE.

The MFP is installed in a general office environment, and its variety of usage methods includes copying, printing, and scanning. Handled documents have a wide range of required secrecy from low confidential to high confidential. TOE security functions offer protection from exposure of highly confidential document data contained in the MFP during the use of a specific function in the MFP. The specified functions are described below.

- **Secure Print Function**

  This function prints the appropriate print data when a password input by the MFP operation panel matches the set password, for print data set a password by a client PC and sent to the MFP and queued in print standby status.

- **Box Function**

  This function controls access to a “box” that is set up as temporary storage area for scan data.

- **Memory Recall Off Copy Function**

  This function always automatically deletes after completion of printing the copy data that is in a condition that would allow reprinting after executing of a copy.

This ST is a document that describes the necessity and sufficiency of TOE security functions offered for the Secure Print Function, the Box Function, and the Memory Recall Off Copy Function.

1.5. Terminologies

This section describes terminology that has particular meaning in this ST.

Job

Operational unit for a series of functions in the MFP, such as the Copy Function, Scan Function, and Print Function etc.

Secure Print

A form of printing when printing from a client PC. When a password is set by the printer driver on a client PC, and printing data is transmitted to MFP, the printing is not executed but rather is queued in standby condition at the MFP. When a set password is entered at the MFP, the standby condition is cancelled and printing is executed.

Secure print job information data

Print data received by the MFP for secure print. This ST handles this as a protected asset.

Job ID

A control number assigned at the MFP to all jobs in a series, starting with secure print jobs.

Box

A directory set as a storage area in the MFP for scanned image data when the HDD is loaded. Individual users can set the name and password only from a client PC. The box indicated as "Public" is shared, so a password cannot be set. A name change cannot be carried out either.

Box Identifier

A name set to the box.

Box Data

Image data stored in the box. The ST handles this as a protective asset.

Box Password

A password set for the individual box. 95 ASCII codes can be used.

Box Utility

A dedicated application for accessing boxes from a client PC. Using this application enables preview display, box data back up by administrator operation, and the restore operation.

Memory Recall Copy/Memory Recall Off Copy

The Copy Function that is always available for reprint after executing printing of a copy is called Memory Recall Copy. On the other hand, the function automatically deleting image data of a scanned document after printing is called Memory Recall Off Copy.

Copy Job Information Data File

Image data scanned into the MFP for use by the Copy Function. This ST handles copy job information data set by Memory Recall Off as protected assets.

Memory Recall Setting Data

Data sets active/inactive status for Memory Recall Copy. Administrators make this setting. When this data is set to OFF, the Memory Recall On Copy/Memory Recall Off Copy selection function offered to the user is no longer offered to the general user. When a copy is executed, the Copy Function operates as Memory Recall Off Copy that automatically deletes the image data of the scanned documents after printing.

SMTP Server Setting Data File

Setting information data files that are related to SMTP server installed in the required MFP environment for transmission of Box data as e-mail. Registration in MFP is required, and secondary asset classification is used for protection of Box data.

FTP Server Setting Data File

Setting information data files that are related to FTP server installed in the required MFP environment for transmission of Box data to the FTP server. Registration in MFP is required, and secondary asset classification is used for protection of Box data.

Administrator Mode

Functions that are provided for authenticated administrators only.

Administrator Mode Password

Passwords set for the administrator mode. Eight-digit numbers can be set.

Service Mode

Functions that are provided for authenticated service engineers only.

Service Code

Passwords that are set for the service mode.

Eight-digit numbers and “*” and “#” can be used.

Unauthorized Access Lock Function

A function for which the operation setting is managed by the administrator. When this function is valid, the box authentication function operates and a series of unsuccessful authentication attempts is detected for each of the authentication functions for the administrator function, secure Print Function and Box Function, and depending on the number of unsuccessful authentications, it locks each authentication function.

Unauthorized Box Access Detection Count value

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the box authentication function while the Unauthorized Access Lock Function is operating.

Unauthorized Secure Print Access Detection Count value

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the secure print authentication function while the Unauthorized Access Lock Function is operating.

Unauthorized Administrator Mode Access Detection Count value

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the administrator authentication function while the Unauthorized Access Lock Function is operating.

Unauthorized Service Engineer Access Detection Count value

A value that is counted and stored as the number of unsuccessful trials, when an authentication trial fails for the service engineer authentication function. Unlike other unauthorized access detection count values, it does not rely on the operational setting of the Unauthorized Access Lock Function.

Access Lock Release Function

A function that clears the unauthorized access detection count value for a box and the unauthorized access detection count value for secure print to zero. When the authentication function for a box and secure print are locked, execution of this function unlocks them.

HDD Lock Function

Security function that is implemented in the HDD used by MFP. A password for accessing the HDD (HDD lock password) can be set, and when this function is used, the authentication function using the HDD lock password operates. Access is not allowed unless the HDD is verified as the MFP. In addition, if the prescribed number of unsuccessful attempts is detected, the authentication function is locked thereafter, and access is completely prohibited.

Auto Reset Function

This function returns to the basic screen at starting of power if access is by the MFP operation panel, when no operation has been detected within the prescribed period. The function intercepts the connection if it’s an access to administrator mode from a client PC.

Auto Reset Operational Settings Data

Time data-enabling setting of Auto Reset Function operations. Can be set to “No limit” or in 1 min increments from 1 to 9 minutes. For administrator mode access from a client PC, operations by time are shown in Table 1.

2. TOE Description

2.1. TOE Type

The #4036 Multi-Function Peripheral Control Software that is the TOE is a software product that comprises a portion of the #4036 MFP control software that is loaded on the MFP. More specifically, it is comprised of the "Macro System Controller" that executes operational control from the MFP operations panel, job resources management, and job sequences control, and the "Network Module" that executes operational control from the client PC.

2.2. Environment for the usage of MFP

The expected general environment for usage is shown in Figure 1.

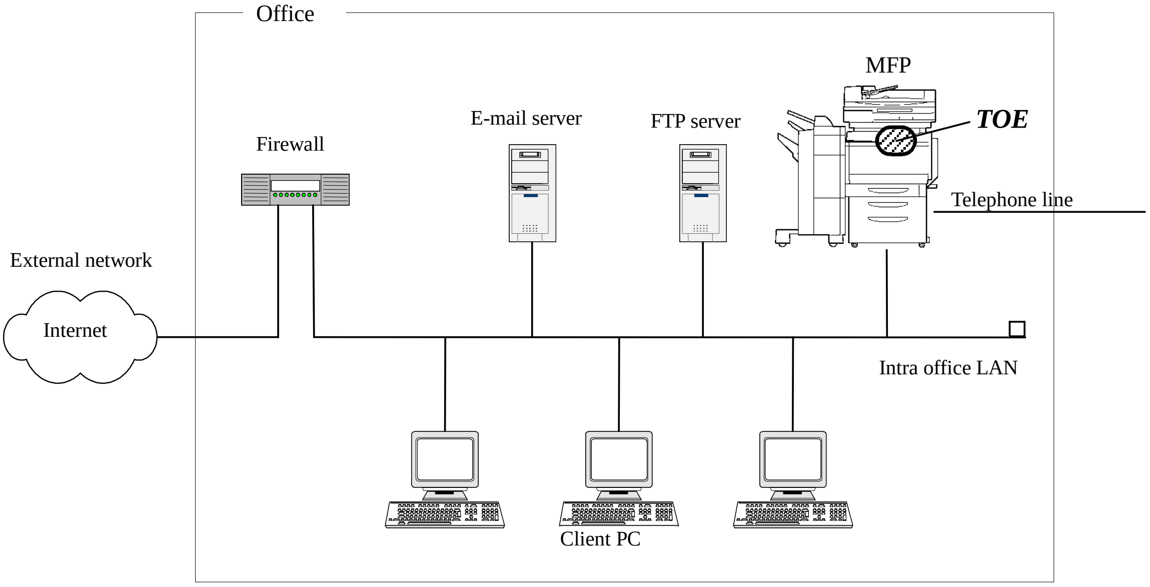


Figure 1 An example of the expected environment for usage of the MFP

As described in the above-mentioned figure, the MFP is installed in a general office. The office will have an operations management system that only allows personnel who are involved in the usage, operation and maintenance of the MFP to enter the room. An intra-office LAN exists as a network in the office. The MFP connects to the client PCs via the intra-office LAN, and has mutual data communication. When an e-mail server and FTP server are connected to the intra-office LAN, the MFP can carry out data communication by using these[2]. When the intra-office LAN connects to an external network, measures such as connecting via a firewall are taken, and an appropriate setup to block access requests to the MFP from the external network is carried out. In addition, by using a switching hub and office operation, the intra-office LAN provides a network environment where the communication data between the MFP and the client PC cannot be intercepted. The MFP is connected to a telephone line in order to communicate with the support center that carries out the maintenance and management of the MFP.

2.3. Role of the TOE User

The roles of the users that relate to the use of the TOE are defined as follows.

- **General User**

  Personnel from the organization that use the MFP, who are allowed to enter the office where the MFP is installed. These personnel can use the general user function that is described in 2.5.1.

- **Administrator**

  Personnel from the organization that use the MFP, who are allowed to enter the office where the MFP is installed, and who carry out the management of the operation. An administrator can use general user functions as a general user, for which details are described in 2.5.1, as well as use the administrator functions described in 2.5.2.

- **Service Engineers**

  Personnel who perform management of the maintenance for the MFP, who are allowed to enter the office where the MFP is installed. These personnel perform machine maintenance (physical maintenance) of the printing engine, etc., of the MFP, and they are able to use the service engineer functions that are provided for management of maintenance functions to adjust each setting, etc. (See 2.5.3.) These personnel are not from the organization, so they are not involved in the operation of the MFP. These maintenance operations are performed under the monitoring of an administrator, preventing unauthorized activities.

- **Person in charge at the Organization that uses the MFP**

[2] <Supplement: E-Mail server and FTP server>
Some office environments where the MFP is installed may not have an e-mail server or FTP server. Also, there may be cases in which there is no connection to an external network or telephone line. In these cases, functions that relate to e-mail, an FTP server or a FAX cannot be used.

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

- **Person in charge at the Organization that manages the Maintenance of the MFP**

A person in charge at the organization that carry out management of the maintenance for the MFP. This person assigns service engineers who perform the maintenance management for the MFP.

2.4. Operational Environment of the TOE

2.4.1. Hardware Environment of the TOE

The TOE hardware environment structure is shown in Figure 2. The TOE is included in the MFP Control Software of the MFP controller. The MFP controller is loaded into the MFP body hardware. An operation panel and network unit is standard installations in the MFP body hardware. In addition, a data controller (required hardware for remote diagnostic functions; see 2.5.4), an HDD with hard disk lock function etc. are installed in the MFP body hardware.

The HDD Lock Function is the function that requires a set password (HDD lock password) for access to data on the hard disk drive. In addition, its function detects unsuccessful attempts to match the hard disk drive lock password, and after detecting a prescribed number of unsuccessful attempts, it has a function to lock the matching function. Accordingly, even if the HDD is stolen, this protects against unauthorized access and preserves confidentiality.

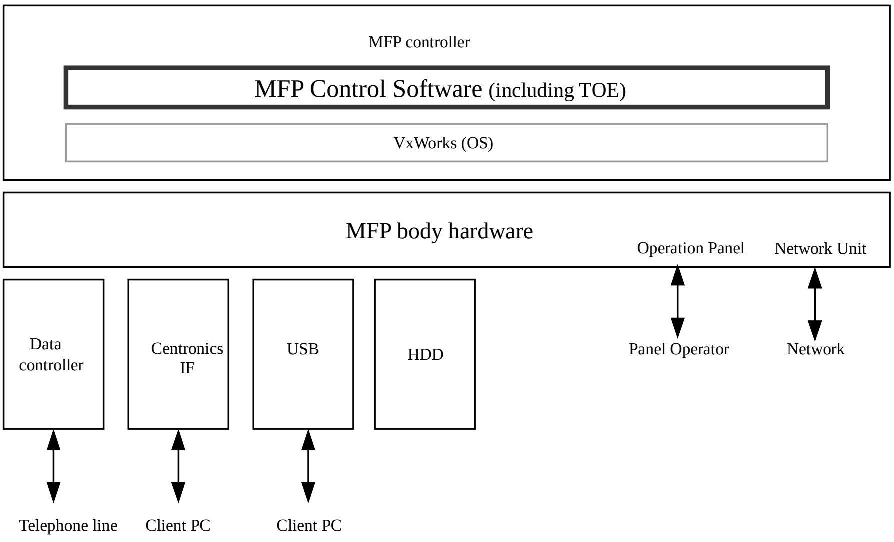


Figure 2 Hardware structure of the TOE

2.4.2. Software Environment of the TOE

The “Macro System Controller” and the “Network Module” that are the TOE operate on the OS (VxWorks) that runs on the MFP controller in the MFP body as object code that is integrated with other MFP control software components. Figure 3 shows the structure of these MFP control software components. The physical area of the TOE is indicated in the dark color in the figure.

The operation overview of each software component including the TOE is described as follows.

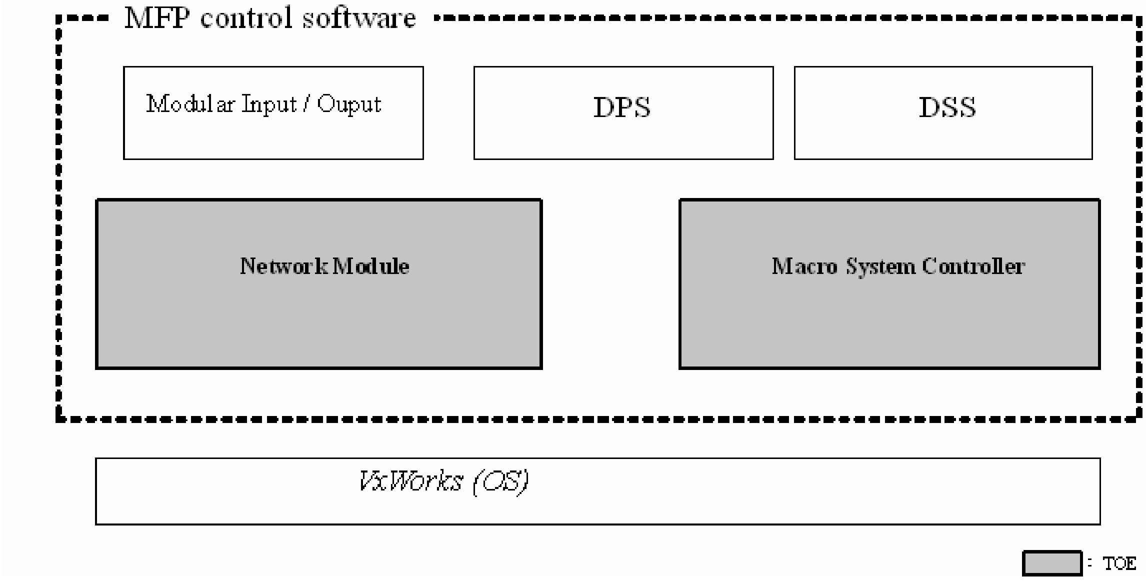


Figure 3 Structure of the MFP control software components

- *VxWorks (OS)*

This is the basic software component required for operation of the MFP control software. It is an operating system. It provides services such as network functions, file system functions and multi-processing for the MFP.

- **<u>Macro System Controller (MSC)</u>**

TOE. A module that registers scanned image data as jobs, and manages job resources, start-up and sequences. It processes input data for LCD, LED and keys used on the MFP body operation panel, and notifies other software components according to processing. It processes messages from others software components and notifies other software components, and it displays data in the MFP body operations panel.

- Modular Input Output (MIO)

  A software component that converts the data received from a variety of external interfaces (network unit, Centronics I/F) to data that is handled by “DPS,” “DSS,” “Network Module,” and “Macro System Controller.” It realizes a WWW server function. In addition, it carries out a variety of network setting processes for IP address, etc.

- **Network Module (NM)**

  TOE. A software component that receives the data from “Modular Input Output”, and processes and controls the data by responding to operation requests from the client PC. Depending on the process, it requests processing to “VxWorks,” or “Macro System Controller”. Also, it receives the data that is processed by “VxWorks,” and “Macro System Controller” and then requests processing to “Modular Input Output.”

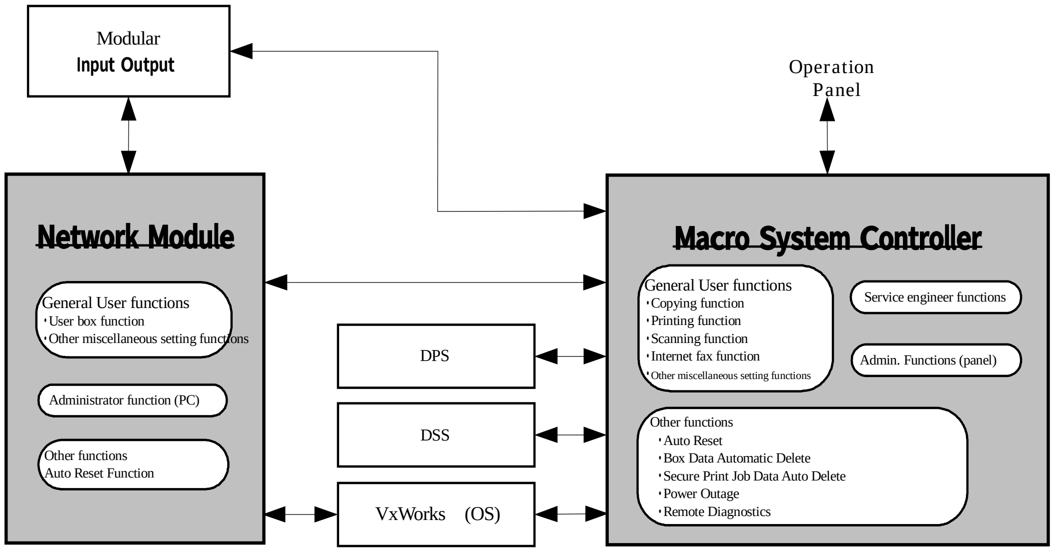
- DPS

  An application software component that executes print reception processing from a client PC.

- DSS

  An application software component that executes processing of e-mail transmissions and FTP transmission of images read by scan.

Accordingly, the “Macros System Controller” and “Network Module” that are the TOE have relationships with other MFP control software components and the OS as shown in the following figure. The details of functions offered by the TOE as shown in the figure will be described in the following section.



*

Figure 4 MFP control software components that relate to the TOE operation processes

2.5. Functions provided by the TOE

General users and administrators use a variety of functions of the MFP built into TOE from a client PC and the operations panel of the MFP body. A service engineer can use the functions for service engineers from the operations panel of the MFP body. The following sections describe **General User Functions** that general users and administrators operate, a variety of functions in the administrator mode that can be operated only by administrators (**Administrator Functions (Panel), Administrator Functions (PC))** and a variety of functions for service engineers (**Service Engineer Functions**).

2.5.1. General User Functions

(1) Copying Function

This function prints image data after spooling the image data to volatile memory when a document is scanned by the MFP body operation panel.

1) Memory Recall Copy

This Copy Function enables limitless reprinting for printable job data remaining after printing when a copy is executed.

2) Memory Recall Off Copy

   This Copy Function automatically deletes job data after printing when a copy has executed. The function is active for execution of automatic deletion based on the settings of the administrator, not the settings of the user, and when a user designates automatic deletion.

3) Scan to Memory (Copy)

   This Copy Function retains print standby status when a copy is executed after selecting scan to copy at execution of a copy. This function is used when a job is combined for printing with another job through the Job Bind Function (described later). Access restrictions are not set for print execution operations of a job that has print standby status.

(2) Printing Function

When print data is transmitted to the MFP using the printer driver of the client PC, the MFP prints the print data received via volatile memory. The Print Function includes the following printing methods.

1) Normal Print
   A Print Function that prints the received print data via the MFP memory as is.

2) Reprint
   A Print Function that allows re-printing or re-printing with different settings such as a print finishing, so that when "reprint" is selected by the client PC, the print data is stored in memory after printing of the print data is completed. There is no specific access limit during the print execution operation.

3) Secure Print
   When a document with high confidentiality is printed, "Secure" is selected from the printer driver of the client PC, the password is set and the print data is sent to the MFP. When the TOE receives the print data, the data is registered as secure print job information data and enters print standby status. The TOE verifies the password entered from the MFP body operations panel with the password of the secure print job information data, when they match, standby status is released and printing is executed. The secure print job information data that has completed printing will be automatically deleted.

4) HDD Store print
   A function that stores the print job information data in the HDD of the MFP. Printing can be done by operating the MFP body operations panel. There is no particular access limit for the operation of print execution.

(3) Job Bind Function

This function selects jobs with print standby status for memory recall copy or reprint, sets the sequence, and prints them as a single job. The TOE executes reception processing for job selection and print execution using this Job Bind Function.

(4) Scanning Function

This function executes scanning from the MFP body operations panel and stores the image as data. There is several data transmission methods for the scanned image data stored in volatile memory such as e-mail and FTP, and they are used by operate simultaneously with the scanning. The image data can be stored in the box of the HDD that is built in the MFP at the time of scanning, without sending it outside MFP.

(5) Internet Fax Function

A function that receives and prints Internet faxes (e-mail with a standard attached image format). Also, it is a function that converts the scanned image data in the MFP to an attachment in an Internet Fax standard image compression format and sends e-mail.

(6) Box Function

Using the web browser of the client PC, it creates a box, where the scanned image data will be stored, (new setting for the name, and password) in HDD and provides the following operations for the box* where the image data (hereafter, “box data”) is stored using the web browser of the client PC.

- Downloading the box data to the client PC
- Deletion of box data
- Deletion of box
- Change in settings for the box (name change, password change)

** There is a default box that is named “public.” “Public” is a shared storage area for general users and operations such as a password setting, a name change or a box deletion cannot be performed.*

In addition, the following operations are offered for scan data stored in the box by the MFP body operations panel.

- Email transmission of the box data to the client PC

- FTP transmission of the box data to the client PC
- Change of box name
- Deletion of box name

The following operations are offered for boxes by using dedicated applications (box utilities) from the client PC.

- Preview display of box data
- List display of the box data (with thumbnails)
- Download of the box data to client PC
- Name change of box data
- Deletion of box data

(7) Other Miscellaneous Setting Functions

In addition to the above-mentioned (1) to (6), there are a multiplicity of functions that carry out a variety of settings such as for Paper Select, Image Quality Select, and Zoom, etc., during printing which are operated from the MFP body operations panel, as functions for the general user. Furthermore, multiple functions, which carry out the viewing of the system status (device structure and outline) of the MFP, the viewing of the job status, the transmission method for the scanning function, and the setting of destination, etc., are available as functions that can be operated using a web-browser from the client PC.

2.5.2. Administrator Function

The TOE provides a management function (administrator function) that supervises general user functions with the administrator mode that is available only for the administrator. The following are descriptions for two categories: the administrator functions (panel) that is management function that can be executed from the MFP body operations panel, and the administrator functions (PC) that is management function that can be executed from a client PC. Also, the administrator functions (box utility) that are the management function that can be used with box utility that is dedicated application from the client PC is described.

(1) Panel Administrator Functions

- Administrator Mode Password Change Function

- Operational Settings Function for Unauthorized Access Lock
- Access Lock Release Function (A function that clears the unauthorized access detection count value for secure printing and for a box to zero.)
- Operational Settings Function for Auto Reset Function (See section 2.5.4)
- HDD Lock Operational Settings Function
- SMTP Server / FTP Server Operational Settings Function
- Settings Function for Memory Recall Settings Data
- A variety of setting functions for the administrator (settings of the storage period for secure print job information data, a variety of settings for a network, settings for limiting the number of copies, settings for date and time, etc.)

(2) PC Administrator Functions

- Deletion of box data
- Deletion of box
- Change in settings for a box (name change, password change)
- Operational Settings for Auto Reset Function
- SMTP server / FTP server operational settings function
- Settings function for memory recall settings data
- A variety of setting functions for administrators (setting of the storage period for box data, setting of the storage period for secure print job information data, a variety of settings for a network, settings for limiting the number of copies, settings for date and time, etc.)

(3) Box Utility Administrator Functions

- Backup function of box data
- Restore function of backup box data

2.5.3. Service Engineer Function

The TOE provides a management function (service engineer function) for general user functions and administrator functions in service mode that can only be operated by a service engineer from the MFP body operations panel. The present functions are described as follows.

- ROM version display function
- Initialization function for administrator mode password
- Function to change the service code
- A variety of setting functions for service engineers (operation setting function for each setting function provided for general users, settings for the counter for the number of pages to be printed, operational checks for each function, a sensor check, settings for an HDD installation, the HDD format, etc.)

2.5.4. Other Functions

The TOE offers functions that operate automatically according to settings of each user, besides functions that operate by direct operation of general users, administrators, and service engineers. The representative functions of this type are described as follows.

(1) Auto Reset Function

This function automatically resets to the basic screen when continued non-operation of the unit exceeds the set period. This function is activated by access from the MFP body operations panel or during access to the administrator mode from a client PC. Administrators set (auto reset setting data). the time to activation of the function (See 2.5.2)

(2) Box Data Automatic Deletion Function

This function deletes box data that has exceeded the set storage period. Administrators set the storage period. (See 2.5.2)

(3) Secure Print Automatic Deletion Function

This function deletes secure print job information data that has exceeded the set storage period. Administrators set the storage period. (See 2.5.2)

(4) Power Save Function

This function automatically regulates the temperature of the print engine fuser heater and saves electrical power in the ways listed below when continued non-operation of the unit exceeds the set period. When the function operates, jobs registered as print standby status are deleted. General users set the period to that is to elapse before activation of this function.

- Preheat Function: Reduces temperature of the print engine fuser heater
- Sleep Function: Turns off print engine fuser heater

(5) Remote Diagnostics Function

This function receives access requests from the support center and transmits to the support center information regarding MFP trouble generation frequency, values showing consumption levels for consumable parts, and print counts. It also automatically accesses the support center and transmits MFP failure information when specified failures (major failures) occur in the MFP. A telephone line and e-mail are used with this function for data sending and receiving.

2.6. Details of the security functions provided by the TOE

In this section, the functions that are related to assets to be protected (copy job information data, secure print job information data, box data) will be described in particular from among the functions of the TOE described in the previous section.

2.6.1. Security function for general user functions

The general user functions listed below are functions that consider security for preventing exposure of document data. Details are as follows.

➢ Function to protect remaining copy data by the Memory Recall Off setting

This function automatically deletes copy job information data scanned by the copy function after printing when Memory Recall Copy has been set by administrator function not to activate.

➢ Identification and authentication that allows access by a general user to a secure print job

A function that identifies and authenticates that a general user is a valid user for secure print job information data when the secure print job data is printed. After failing three times at authentication, it locks the authentication function for the concerned secure print job information data and access is denied.

When authentication is successful, the concerned secure print job information data starts to be printed.

➢ Function to create a box

A function by which a general user specifies a name and creates a box.

➢ Identification and authentication that allows access to a box by a general user and an access control function

A function that identifies and authenticates that a general user is an authorized user of a box when accessing the box. After failing three times at authentication, it locks the authentication function for the concerned box and access is denied.

When authentication is successful, the downloading of all the box data in the box is permitted. (The box named as "Public" is not subject to the present security function.)

➢ Box management function for general users whose access is authenticated

A function by which a general user, who is a valid user of the box, can change the settings (name, password) of the box.

Functions related to deletion of secure print job information data and box data are not considered as security functions because threats are not assumed for the following reasons:

- There is no intention for a long-term storage.
- Availability of data falls by voluntary deletion, but there is no need to consider this because the original data and printing are controlled and stored by each user.

2.6.2. Security functions for the administrator functions

There are management functions that involve assets to be protected from among the administrator functions. The access to this administrator function including the management function is limited to those authenticated by the administrator mode password by using a password that could only be known by the administrator. The identification and authentication functions and the management functions that are related to the protected assets, which can be operated after authentication, are security functions. The details are described as follows.

➢ Identification and authentication function that allows access to the administrator mode

- This function identifies and authenticates the administrator when accessing the administrator mode using the MFP body operations panel or using a web-browser on the client PC. Failing three times locks the authentication function and access is denied.

- This function authenticates the administrator when using a box utility from a client PC to execute the back up function or the restore function for box data. As with the above function, if failure occurs three times, the administrator authentication function locks and access is denied.

➢ Security-related functions for administrator mode

The following functions enable operation from the MFP body operations panel in administrator mode.

- Administrator Mode Password Change Function

- Operational setting function for Unauthorized Access Lock

- Access Lock Release Function

- Operational Settings Function for Auto Reset Function

- SMTP Server / FTP Server Settings Function

- Settings Function for Memory Recall Settings Data

The following functions can be operated from the client PC in administrator mode.

- Function to change the setting of the box (name change, password change)

- Operational Settings Function for Auto Reset Function

- SMTP Server / FTP Server Settings Function

- Settings Function for Memory Recall Settings Data

2.6.3. Security Functions for Service Engineer Function

Some of the service engineer functions for the service mode are management functions that involve assets to be protected. The access to the service mode, including these management functions, is limited to those authenticated by the service code, by using a password that could only be known by the service engineer, along with undisclosed secret information that could only be known by the service engineer. The identification and authentication functions and the management functions that are related to the protected assets, which can be operated after authentication, are security functions. The details are described as follows.

- <u>Identification and authentication function that allows access to the service mode</u>

  A function that authenticates the service engineer when accessing the service mode. Failing three times locks the authentication function and access is denied.

- <u>Security-related functions for service engineer mode</u>

  The following functions allowing operation in service mode.

  - Initialization function for the administrator mode password.
  - Function to change the service code.

2.6.4. Security Functions for Other Functions

The Auto Reset Function returns to the MFP body panel basic screen or interrupts the connection if the connection has been made from a PC client when non-operation continues. Accordingly, it is effective as a supplementary security function for case where the operator leaves their station inadvertently at the time of accessing administrator mode. Details are described below.

- Auto Reset Function

This function cancels access permission when non-operation has continued for a set period. The administrator sets the operating period for this function to a period shown in the table below.

Table 1. Operational Settings and Behavior for Auto Reset Function

Access Condition Operation Period	Operation for Administrator Mode accessed from MFP unit operation panel	Operation for Administrator Mode accessed from client PC
Off	Does not operate	Operates after 10 minutes
1, 2, 3, 4, 5 min.	Operates as set for 1, 2, 3, 4, 5 min.	Operates after 5 minutes (fixed)
6, 7, 8, 9 min.	Operates as set for 6, 7, 8, 9 min.	Operates as set for 6, 7, 8, 9 min.

3. TOE Security Environment

This chapter will describe the assumptions, threats, and organizational security policies.

3.1. Assumptions

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

A.ADMIN (Personnel conditions to be an administrator)

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

A.AUTH (Operation conditions for passwords)

Each password used for using the TOE will be managed so that it will not be divulged by the owner of the password.

A.HDD (Hardware environment condition used by MFP)

- Only HDD that have a hard disk lock function is used in the MFP that includes the TOE.
- HDD lock passwords used with the HDD lock function must not be leaked or revealed by anyone who has one or more of these passwords.

A.NETWORK (Network connection conditions for MFP)

- The organization that uses the MFP will construct a network environment for an intra-office LAN where the MFP will be installed, which will not be intercepted.
- When the intra-office LAN where the MFP with the TOE will be installed is connected to an external network, access from the external network to the MFP is not allowed.

A.PHYSICAL (Installation conditions for the MFP)

The MFP where the TOE is loaded will be installed in a place where it is physically protected and where only the general users, administrator and service engineer are permitted to enter.

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

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

A.SETTING (Security functions operational setting conditions)

TOE users will use the TOE in a condition in which the Unauthorized Access Lock Function always operates.

3.2. Threats

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

T.ACCESS-SECURE-PRINT (Unauthorized operation of the secure print job information data)

Unauthorized exposure of secure print job information data when a malicious general user accesses the secure print job information data from the MFP body operations panel and prints the data that was sent by another user.

T.ACCESS-BOX (Unauthorized operation of the box data)

- Unauthorized exposure of box data when a malicious general user accesses the created box from a client PC and downloads, previews, or displays as thumbnails for the box data of a box used by another general user.
- Unauthorized exposure of box data when a malicious general user accesses the created box from the MFP body operation panel and transmits by email or FTP the box data of a box used by another general user.
- Unauthorized exposure of box data when a malicious general user accesses the created box from a client PC and backs up the box data.
- Unauthorized falsification of box data when a malicious general user accesses the created box from a client PC and restores backed up box data.

T.ACCESS-COPY-DATA (Unauthorized operation to the remaining copy job information data)

Unauthorized exposure of copy job information data when a malicious general user accesses the copy job information data by the MFP body operation panel and reprint it.

T.SEND-BOX-DATA (Transmission of box data to an address not assumed)

- Exposure of box data by inadvertent transmission to a server not intended by the general user when a malicious general user accesses from the MFP body operation panel and changes settings data for the SMTP server or FTP server used by the MFP.
- Exposure of box data by inadvertent transmission to a server not intended by the general user when a malicious general user accesses from a client PC and changes settings data for the SMTP server or FTP server used by the MFP.

3.3. Organizational Security Policies

P.BEHAVIOR-FUNCTION (Operation settings function for security function)

- In a secure environment, it is capable of deactivating the Unauthorized Access Lock Function in order to design convenience for operation.
- In a secure environment, it is capable of activating the Memory Recall Copy Function in order to design convenience for operation.

4. Security Objectives

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

4.1. Security Objectives for the TOE

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

O.ACCESS-ADMIN (management function operated by an administrator)

The TOE permits execution of the operation of administrator functions for the administrator only.

O.ACCESS-BOX (box access control)

- The TOE permits execution of box data downloading, preview, thumbnail display, e-mail transmission, and FTP transmission for general users who are authorized users.

- The TOE permits execution of box data downloading (backup operation) and uploading (restore operation) for all boxes only to administrators.

O.ACCESS-SECURE-PRINT (Secure print job access control)

The TOE permits secure print job information data printing operations only for general users who are authorized users.

O.ACCESS-SERVICE (management function operated by a service engineer)

The TOE permits execution of operation of the service engineer functions only for service engineers.

O.CONTROL-COPY (Copy Function operation control)

The TOE deletes scanned copy job information data by the use of Copy Function after printing has completed.

O.I&A-ADMIN (identification and authentication of an administrator)

The TOE identifies and authenticates whether the user accessing the administrator function from the client PC or the MFP body operation panel is an administrator.

O.I&A-SERVICE (identification and authentication of a service engineer)

The TOE identifies and authenticates whether the user who accesses the service engineer function from the MFP body operations panel is a service engineer.

O.I&A-USER (identification and authentication of a general user)

The TOE identifies and authorizes whether the user who accesses the secure print job information data or box data is a general user who is a valid user.

4.2. Security objectives for the Environment

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

4.2.1. IT environment security objectives

OE.FEED-BACK (password feedback)

Box utilities used by the client PC offer protected appropriate feedback for an input box password or administrator mode password.

OE.SECURE-PRINT-QUALITY (quality metrics for secure print job password)

The printer driver of the client PC adds a password, of which the strength is assured, to the print data that is sent to the MFP as a secure print.

4.2.2. Non-IT environment security objective

OE-N.ADMIN (Reliable Administrator)

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

OE-N.AUTH (Proper Management and Password Usage)

- The administrator shall have general users execute the following operations.

  - General users shall keep the secure print password and box password confidential.

  - General users shall not use a secure print password and box password that can be easily guessed.

  - General users shall appropriately change the box password.

- The person in charge in the organization using the MFP shall have the administrator execute the following operations.

  - Administrator shall not use an administrator mode password that can be easily guessed.

  - Administrator shall keep the administrator mode password confidential.

  - Administrator shall appropriately change the administrator mode password.

  - Administrator shall always carry out the modification operation when the administrator mode password is initialized.

- The person in charge in the organization managing maintenance of the MFP shall have the service engineer execute the following operations.

  - Service engineer shall not use a service code that can be easily guessed.

  - Service engineer shall keep the service code confidential.

  - Service engineer shall appropriately change the service code.

OE-N.HDD (HDD Used by the MFP)

- Service engineers shall install an HDD having HDD Lock Function into the MFP loaded with the TOE.

- The person in charge in the organization using the MFP shall have administrators operate as follows.

  - Administrator shall not use an HDD lock password that can be easily guessed.

  - Administrator shall keep the HDD lock password confidential.

  - Administrator shall appropriately change the HDD lock password.

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

- The administrator shall install devices that realize a network environment for the office LAN where the MFP with the TOE is installed that cannot be intercepted, and execute an appropriate setting that does not allow interception.

- The administrator shall install devices that block access to the MFP with the TOE from an external network, and execute an appropriate setting to block access.

OE-N.PHYSICAL (Environment for MFP Installation)

The administrator shall install the MFP with the TOE in a physically protected office, and execute operation management where only the general users, administrator, and service engineer can enter the office.

OE-N.SERVICE (Reliable Service Engineer)

The person in charge of the organization that carries out the maintenance management of the MFP shall assign a person who will faithfully carry out the given role for the installation of the TOE and the maintenance of the MFP with the TOE as a service engineer.

OE-N.SESSION (Termination of Session After Use)

- The administrator shall have general users always terminate the session after use of the Box Function.

- The administrator shall always terminate the session after use of the administrator function.

- The service engineer shall always terminate the session after use of the service engineer function.

OE-N.SETTING-1 (Security Function Operational Settings 1)

- Administrator shall operate the TOE in a condition that always operates the Unauthorized Access Lock Function.

OE-N.SETTING-2 (Security Function Operational Settings 2)

- Administrator shall operate the TOE in a condition in which the Memory Recall Copy Function is always deactivated.

5. IT Security Requirements

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

5.1. TOE Security Requirements

5.1.1. TOE Security Function Requirements

The security function requirements required for the TOE are described. Those regulated in CC Part 2 will be directly used for all the functional requirements components, and the same labels will be used as well. In the following description, when items are indicated in "italic" and "bold" it means that they are assigned or selected. When indicated in "italic" and "bold" and "underline" it means that they are refined. A number in the parentheses after a label means that the functional requirement is used repeatedly. The label in the parentheses "( )" in the dependent section indicates a label for the security functional requirements used in this ST. When it is a dependency that is not required to be used in this ST, it is described as "N/A" in the same parentheses.

5.1.1.1. User data protection

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

Table 2. Operational List for Secure Print Job Information Data File

Subject	Object	Operational list
Operational processes for secure print jobs	***Secure print job information data files***	***• Print*** ***• Registration***

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

Table 3. Operational List for Box Data File

Subject	Object	Operational list
Operational processes for the box	***Box***	***• Read box data in the box*** ***• Write box data in the box*** ***• Creation***

FDP_ACC.1[3]	**Subset access control**
FDP_ACC.1.1[3]	

The TSF shall enforce the [assignment: *access control SFP*] on [assignment*: list of subjects, objects, and operations among subjects and objects covered by the SFP*]. [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]: ***Listed in "Table 4 Operational List for Copy Job Information Data File"*** [assignment: *access control SFP*] ***Copy job access control***	
Hierarchical to:	No other components
Dependencies:	FDP_ACF.1 (FDP_ACF.1[3])

Table 4. Operational List for Copy Job Information Data File

Subject	Object	Operational list
Operational processes for copy job	***Copy job information data file***	***• Deletion***

FDP_ACF.1[1]	**Security attribute based access control**
FDP_ACF.1.1[1]	
The TSF shall enforce the [assignment: *access control SFP*] to objects, based on [assignment: *security attributes, named groups of security attributes*].	
[assignment: *security attributes, named group of security attributes*]: ***Job ID***	
[assignment: *access control SFP*]: ***Secure Print Job Access Control***	
FDP_ACF.1.2[1]	
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].	

[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]: • ***When the process operating a secure print job receives a secure print job registration request, a newly assigned "job ID" is created and the secure print job information data file having these object attributes is registered.*** • ***During the process of operating the secure print job having the "job ID" selected by a general user, the print operation is permitted only for secure print job information data files having an identical "job ID".***
FDP_ACF.1.3[1]
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: r*ules, based on security attributes, that explicitly authorize access of subjects to objects*]: ***None***
FDP_ACF.1.4[1]
The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].
[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]: ***None***
Hierarchical to: No other components **Dependencies:** FDP_ACC.1 (FDP_ACC.1[1]), FMT_MSA.3 (FMT_MSA.3[1])

FDP_ACF.1[2] **Security attribute based access control**
FDP_ACF.1.1[2]
The TSF shall enforce the [assignment: *access control SFP*] to objects, based on [assignment: *security attributes, named groups of security attributes*].
[assignment: *security attributes, named groups of security attributes*]: ***Box identifier*** ***Administrator identifier*** [assignment: *access control SFP*]: ***Box access control***

FDP_ACF.1.2[2]

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

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

- ***The process operating the box having a "box identifier" is permitted a "creation" operation for a box having this "box identifier" as an object attribute when there is no box having an identical "box identifier."***
- ***The process operation the box having a "box identifier" is denied a "creation" operation for a box having this "box identifier" as an object attribute when there is a box having a having an identical "box identifier."***
- ***During the process of operating the user box having a "box identifier" selected by the general user, "read box data within a box" operation is permitted only for boxes having an identical "box identifier" as above.***
- ***The process operating boxes having an "administrator identifier" is permitted a "read box data within a box" operations of all boxes.***
- ***The process operating boxes having a "administrator identifier" is permitted a "write box data in a box" operations to all boxes.***

FDP_ACF.1.3[2]

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

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

None

FDP_ACF.1.4[2]

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

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

None

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

FDP_ACF.1[3] Security attributes based access control

FDP_ACF.1.1[3]

The TSF shall enforce the [assignment: *access control SFP*] to objects, based on [assignment: *security attributes, named groups of security attributes*].

[assignment: *security attributes, named groups of security attributes*]:

Memory recall setting data

[assignment: *access control SFP*]:

Copy job access control

FDP_ACF.1.2[3]

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

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

The process operating the copy job executes the delete operation after print completion for copy job information data files wherein "memory recall setting data" is "Off".

FDP_ACF.1.3[3]

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

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

None
FDP_ACF.1.4[3]
The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].
[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]: ***None***
Hierarchical to: No other components **Dependencies:** FDP_ACC.1 (FDP_ACC.1[3]), FMT_MSA.3 (FMT_MSA.3[3])

5.1.1.2. Identification and Authentication

FIA_AFL.1[1] **Authentication failure handling**
FIA_AFL.1.1[1]
The TSF shall detect when [assignment*: number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].
[assignment: *list of authentication events*]: ***Authentication of a general user who is a valid user of the secure print job***
[assignment: *number*]: ***3***
FIA_AFL.1.2[1]
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].
[assignment: *list of actions*]: ***Lock the authentication function of the general user who is a valid user of the corresponding secure print job, unless the following operation to recover the normal condition is executed.***

<Operation for recovering the normal condition> ***Execute the Access Lock Release Function for secure print jobs.***
Hierarchical to: No other components **Dependencies:** FIA_UAU.1 (FIA_UAU.2[1])

FIA_AFL.1[2]	**Authentication failure handling**
FIA_AFL.1.1[2]	
The TSF shall detect when [assignment*: number*] unsuccessful authentication attempts occur related to [assignment: l*ist of authentication events*].	
[assignment: *list of authentication events*]: ***Authentication of a general user who is a valid user of the box.***	
[assignment: *number*]: ***3***	
FIA_AFL.1.2[2]	
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].	
[assignment: *list of actions*]: ***Lock the authentication function of the general user who is a valid user of the corresponding box, unless the following operation to recover the normal condition is executed.*** ***<Operation for recovering the normal condition>*** ***Execute the Access Lock Release Function for the boxes.***	
Hierarchical to:	No other components
Dependencies:	FIA_UAU.1 (FIA_UAU.2[2])

FIA_AFL.1[3] **Authentication failure handling**
FIA_AFL.1.1[3]
The TSF shall detect when [assignment*: number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].
[assignment: *list of authentication events*]: ***Authentication of an administrator.***
[assignment: *number*]: ***3***
FIA_AFL.1.2[3]
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].
[assignment: *list of actions*]: ***Lock the authentication function of the administrator.*** ***<Operation for recovering the normal condition>*** ***There is no function for lock release.***
Hierarchical to: No other components **Dependencies:** FIA_UAU.1 (FIA_UAU.2[3])

FIA_AFL.1[4] **Authentication failure handling**
FIA_AFL.1.1[4]
The TSF shall detect when [assignment*: number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].
[assignment: *list of authentication events*]: ***Authentication of a service engineer.***
[assignment: *number*]:

3

FIA_AFL.1.2[4]

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

[assignment: *list of actions*]:

Lock the authentication function of the service engineer.

<Operation for recovering the normal condition>

There is no function for lock release

Hierarchical to: No other components

Dependencies: FIA_UAU.1 (FIA_UAU.2[4])

FIA_SOS.1[1] Verification of secrets

FIA_SOS.1.1[1]

The TSF shall provide a mechanism to verify that the ***box password*** meets [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]:

Minimum 4 digits, maximum 64 digits ASCII code 0x20 to 0x7E (95 types in English one-byte characters and one byte symbols).

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 the ***administrator mode password*** meets [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]: ***Exact 8-digit number (0 to 9).***
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 the ***service code*** meets [assignment: *a defined quality metric*].
[assignment: *a defined quality metric*]: ***Exact 8-digit number (0 to 9) or "*" or "#."***
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 ***general user who is a valid user of a secure print job*** to authenticate itself before allowing any other TSF-mediated actions on behalf of that ***general user who is a valid user of the secure print job***.
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 ***general user who is a valid user of a box*** to authenticate itself before allowing any other TSF-mediated actions on behalf of that ***general user who is a valid user of a box***.
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 an ***administrator*** to authenticate itself before allowing any other TSF-mediated actions on behalf of that ***administrator***.
Hierarchical to: FIA_UAU.1 **Dependencies:** FIA_UID.1 (FIA_UID.2[3])

FIA_UAU.2[4] User authentication before any action
FIA_UAU.2.1[4]
The TSF shall require each ***service engineer*** to authenticate itself before allowing any other TSF-mediated actions on behalf of that ***service engineer***.
Hierarchical to: No other components **Dependencies:** FIA_UID.1 (FIA_UID.2[4])

FIA_UAU.6 Re-authenticating
FIA_UAU.6.1
The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is required*].
[assignment: *list of conditions under which re-authentication is required*]

- ***Change administrator mode password.***
- ***Change service code.***

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1

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

[assignment: *list of feedback*]:

Display "*" for each character of character data entered as an administrator mode password, service code, box password, or secure print password.

Hierarchical to: No other components

Dependencies: FIA_UAU.1 (FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.2[4])

FIA_UID.2[1] User identification before any action

FIA_UID.2.1[1]

The TSF shall require a ***general user who is a valid user of a secure print job*** to identify itself before allowing any other TSF-mediated actions on behalf of that ***general user who is a valid user of the secure print job***.

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 a ***general user who is a valid user of a box*** to identify itself before allowing any other TSF-mediated actions on behalf of that ***general user who is a valid user of a box***.

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 an ***administrator*** to identify itself before allowing any other TSF-mediated action on behalf of that ***administrator***.

Hierarchical to: FIA_UID.1

Dependencies: No dependencies

FIA_UID.2[4] User identification before any action

FIA_UID.2.1[4]

The TSF shall require a ***service engineer*** to identify itself before allowing any other TSF-mediated action on behalf of that ***service engineer***.

Hierarchical to: FIA_UID.1

Dependencies: No dependencies

5.1.1.3. Security management

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1

The TSF shall restrict the ability to [selection*: determine the behaviour of, disable, enable,*

modify the behaviour of] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].
[assignment: *list of functions*]: ***Unauthorized Access Lock Function*** [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] : ***Enable, Disable*** [assignment: *the authorised identified roles*] ***Administrator***
Hierarchical to: No other components **Dependencies:** FMT_SMF.1 (FMT_SMF.1), FMT_SMR.1 (FMT_SMR.1[3])

FMT_MSA.1[1] **Management of security attributes**
FMT_MSA.1.1[1]
The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment*: list of security attributes*] to [assignment: *the authorised identified roles*].
[assignment: *list of security attributes*]: ***Box identifier*** [Selection: *change_default, query, modify, delete, [assignment: other operations]*] : ***Modify*** [assignment: *the authorised identified roles*] ***General user who is valid user of the box, Administrator*** [assignment: *access control SFP, information flow control SFP*] ***Box access control***

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

FMT_MSA.1[2] Management of security attributes

FMT_MSA.1.1[2]

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

[assignment: *list of security attributes*]:

Memory Recall Settings Data

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

change_default, query

[assignment: *the authorised identified roles*]

Administrator

[assignment: *access control SFP, information flow control SFP*]

Copy job access control

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

FMT_MSA.3[1] Static attribute initialisation

FMT_MSA.3.1[1]

The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [Selection: *restrictive, permissive, other property*] default values for the ***Job ID*** that are used to enforce the SFP.

[Selection: *restrictive, permissive, other property*]:

other property (Value allows unique identification by distinguishing secure print job from other jobs

[assignment: *access control SFP, information flow control SFP*]:

Secure print job access control

FMT_MSA.3.2[1]

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

[assignment: *the authorised identified roles*]:

None

Hierarchical to: No other components

Dependencies: FMT_MSA.1 (N/A), FMT_SMR.1 (N/A)

FMT_MSA.3[2] Static attribute initialisation

FMT_MSA.3.1[2]

The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [Selection: *restrictive, permissive, other property*] default values for the ***Box Identifier*** that are used to enforce the SFP.

[Selection: *restrictive, permissive, other property*]:

Permissive

[assignment: *access control SFP, information flow control SFP*]:

Box access control

FMT_MSA.3.2[2]

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

[assignment: the *authorised identified roles*]:

General user who creates the box

Hierarchical to: No other components

Dependencies: FMT_MSA.1 (FMT_MSA.1[1]), FMT_SMR.1 (FMT_SMR.1[1])

FMT_MSA.3[3] Static attribute initialisation

FMT_MSA.3.1[3]

The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [Selection: *restrictive, permissive, other property*] default values for the ***Memory Recall Settings Data*** that are used to enforce the SFP.

[Selection: *restrictive, permissive, other property*]:

Restrictive

[assignment: *access control SFP, information flow control SFP*]:

Copy job access control

FMT_MSA.3.2[3]

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

[assignment: *the authorised identified roles*]:

None

Hierarchical to: No other components

Dependencies: FMT_MSA.1 (FMT_MSA.1[2]), FMT_SMR.1 (None)

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*]: • ***Administrator mode password*** • ***Auto reset operation settings data***	
[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_SMF.1), FMT_SMR.1 (FMT_SMR.1[3])

FMT_MTD.1[2]	**Management of TSF data**
FMT_MTD.1.1[2]	
The TSF shall restrict the ability to [Selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified data*].	
[assignment: *list of TSF data*]: • ***Box unauthorized access detection count value*** • ***Secure print unauthorized access detection count value***	
[Selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]: ***Clear***	
[assignment: *the authorised identified roles*]: ***Administrator***	
Hierarchical to:	No other components
Dependencies:	FMT_SMF.1 (FMT_SMF.1), FMT_SMR.1 (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*]:

Box password

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

Modify

[assignment: *the authorised identified roles*]:

General user who is valid user of the box, Administrator

Hierarchical to: No other components

Dependencies: FMT_SMF.1 (FMT_SMF.1), FMT_SMR.1

(FMT_SMR.1[2], FMT_SMR.1[3])

FMT_MTD.1[4] Management of TSF data

FMT_MTD.1.1[4]

The TSF shall restrict the ability to [Selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

[assignment: *list of TSF data*]:

Service code

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

Modify

[assignment: *the authorised identified roles*]:

Service engineer	
Hierarchical to:	No other components
Dependencies:	FMT_SMF.1 (FMT_SMF.1), FMT_SMR.1 (FMT_SMR.1[4])

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 mode password***	
[Selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]: ***[assignment: other operations]: Initialization (operation to return to the default)***	
[assignment: *the authorised identified roles*]: ***Service engineer***	
Hierarchical to:	No other components
Dependencies:	FMT_SMF.1 (FMT_SMF.1), FMT_SMR.1 (FMT_SMR.1[4])

FMT_SMF.1 Specification of Management Functions
FMT_SMF.1.1
The TSF shall be capable of performing the following security management functions: [assignment: *list of security management functions provided by the TSF*].
[assignment: *list of security management functions provided by the TSF*]: ***Listed in applicable section of "Table 5 List of Security Management Functions"***

Hierarchical to: No other components

Dependencies: No dependencies

Table 5. List of Security Management Functions

N/A: Not Applicable

Functional Requirement Components	Management Items Listed in CC Part 2	Application
FDP_ACC.1[1]	There are no management activities foreseen for this component.	N/A
FDP_ACC.1[2]	There are no management activities foreseen for this component.	N/A
FDP_ACC.1[3]	There are no management activities foreseen for this component.	N/A
FDP_ACF.1[1]	The following actions could be considered for the management functions in FMT: a) Managing the attributes used to make explicit access or denial based decisions.	There is no management function that is applicable for the management items on the left.
FDP_ACF.1[2]	The following actions could be considered for the management functions in FMT: a) Managing the attributes used to make explicit access or denial based decisions.	There is no management function that is applicable for the management items on the left; however, the following security management functions are specified as related items for the requirement. ● ***Creation function of box identifier*** ● ***Modification function of box identifier (operated by the general user who is a valid user of the box)*** ● ***Modification function of box identifier (operated by the administrator)***
FDP_ACF.1[3]	The following actions could be considered for the management functions in FMT: a) Managing the attributes used to make explicit access or denial based decisions.	There is no management function that is applicable for the management items on the left; however, the following security management functions are specified as related items for the requirement. ● ***Setting function of memory recall data***

Functional Requirement Components	Management Items Listed in CC Part 2	Application
FIA_AFL.1[1]	The following actions could be considered for the management functions in FMT: a) Management of the threshold for unsuccessful authentication attempts: b) Management of actions to be taken in the event of an authentication failure.	There is no management function that is applicable for the management items on the left; however, the following security management functions are specified as related items for the requirement. • ***Operation setting function for the Unauthorized Access Lock Function*** • ***Access Lock Release Function clearing the secure print unauthorized access detection count value***
FIA_AFL.1[2]	The following actions could be considered for the management functions in FMT: a) Management of the threshold for unsuccessful authentication attempts: b) Management of actions to be taken in the event of an authentication failure.	There is no management function that is applicable for the management items on the left; however, the following security management functions are specified as related items for the requirement. • ***Operation setting function for the Unauthorized Access Lock Function*** • ***Access Lock Release Function clearing the box unauthorized access detection count value***
FIA_AFL.1[3]	The following actions could be considered for the management functions in FMT: a) Management of the threshold for unsuccessful authentication attempts b) Management of actions to be taken in the event of an authentication failure.	There is no management function that is applicable for the management items on the left; however, the following security management functions are specified as related items for the requirement. • ***Operation setting function for the Unauthorized Access Lock Function***
FIA_AFL.1[4]	The following actions could be considered for the management functions in FMT: a) Management of the threshold for unsuccessful authentication attempts; b) Management of actions to be taken in the event of an authentication failure.	There is no management function that is applicable for the management items on the left.

Functional Requirement Components	Management Items Listed in CC Part 2	Application
FIA_SOS.1[1]	The following actions could be considered for the management functions in FMT: a) The management of the metric used to verify the secrets.	There is no management function that is applicable for the management items on the left.
FIA_SOS.1[2]	The following actions could be considered for the management functions in FMT: a) The management of the metric used to verify the secrets	There is no management function that is applicable for the management items on the left.
FIA_SOS.1[3]	The following actions could be considered for the management functions in FMT: a) The management of the metric used to verify the secrets.	There is no management function that is applicable for the management items on the left.
FIA_SOS.1[4]	The following actions could be considered for the management functions in FMT: a) The management of the metric used to verify the secrets.	There is no management function that is applicable for the management items on the left.
FIA_UAU.2[1]	The following actions could be considered for the management functions in FMT: Management of the authentication data by an administrator; Management of the authentication data by the user associated with this data.	There is no management function that is applicable for the management items on the left.
FIA_UAU.2[2]	The following actions could be considered for management functions in FMT: Management of the authentication data by the administrator; Management of the authentication data by the user associated with this data.	• ***Modification function for the box password (operated by the general user who is a valid user of the box)*** • ***Modification function for the box password (operated by the administrator)*** • ***Operation setting function for the Unauthorized Access Lock Function***

Functional Requirement Components	**Management Items Listed in CC Part 2**	**Application**
FIA_UAU.2[3]	The following actions could be considered for the management functions in FMT: Management of the authentication data by an administrator. Management of the authentication data by the associated user: Controlling the list of actions that can be taken before the user is authenticated.	***• Modification function for the administrator mode password*** ***• Initialization function for the administrator mode password***
FIA_UAU.2[4]	The following actions could be considered for the management functions in FMT: Management of the authentication data by an administrator; Management of the authentication data by the user associated with this data.	***• Modification function for the service code***
FIA_UAU.6	The following actions could be considered for the management functions in FMT. If an authorised administrator could request re-authentication, the management includes a re-authentication request.	There is no management function that is applicable for the management items on the left.
FIA_UAU.7	There are no management activities foreseen.	N/A

Functional Requirement Components	**Management Items Listed in CC Part 2**	**Application**
FIA_UID.2[1]	The following actions could be considered for the management functions in FMT: a) Management of the user identities.	There is no management function that is applicable for the management items on the left.

Functional Requirement Components	**Management Items Listed in CC Part 2**	**Application**
FIA_UID.2[2]	The following actions could be considered for the management functions in FMT: a) Management of the user identities.	***• Creation function of box identifier*** ***• Modification function of box identifier (operated by the general user who is a valid user of the box)*** ***• Modification function of box identifier (operated by the administrator)***
FIA_UID.2[3]	The following actions could be considered for the management functions in FMT: a) The management of the user identities.	There is no management function that is applicable for the management items on the left.
FIA_UID.2[4]	The following actions could be considered for the management functions in FMT: a) The management of the user identities.	There is no management function that is applicable for the management items on the left.
FMT_MOF.1	The following actions could be considered for the management functions in FMT management: a) Managing the group of roles that can interact with the functions in TSF.	There is no management function that is applicable for the management items on the left.
FMT_MSA.1[1]	The following actions could be considered for the management functions in FMT management: a) Managing the group of roles that can interact with the security attributes.	There is no management function that is applicable for the management items on the left.
FMT_MSA.1[2]	The following actions could be considered for the management functions in FMT management: a) Managing the group of roles that can interact with the security attributes.	There is no management function that is applicable for the management items on the left.

Functional Requirement Components	Management Items Listed in CC Part 2	Application
FMT_MSA.3[1]	The following actions could be considered for the management functions in FMT management: a) Managing the group of roles that can specify initial values. b) Managing the permissive or restrictive setting of default values for given access control SFP.	There is no management function that is applicable for the management items on the left.
FMT_MSA.3[2]	The following actions could be considered for the management functions in FMT management: a) Managing the group of roles that can specify initial values. b) Managing the permissive or restrictive setting of default values for given access control SFP.	There is no management function that is applicable for the management items on the left.
FMT_MSA.3[3]	The following actions could be considered for the management functions in FMT management: a) Managing the group of roles that can specify initial values. b) Managing the permissive or restrictive setting of default values for given access control SFP.	There is no management function that is applicable for the management items on the left.
MFT_MTD.1[1]	The following actions could be considered for the management functions in FMT management: a) Managing the group of roles that can interact with the TSF data.	There is no management function that is applicable for the management items on the left.
FMT_MTD.1[2]	The following actions could be considered for the management functions in FMT management: a) Managing the group of roles that can interact with the TSF data.	There is no management function that is applicable for the management items on the left.

Functional requirement components	Management items listed in CC Part 2	Application
FMT_MTD.1[3]	The following actions could be considered for the management functions in FMT management: a) Managing the group of roles that can interact with the TSF data.	There is no management function that is applicable for the management items on the left.
FMT_MTD.1[4]	The following actions could be considered for the management functions in FMT management: a) Managing the group of roles that can interact with the TSF data.	There is no management function that is applicable for the management items on the left.
FMT_MTD.1[5]	The following actions could be considered for the management functions in FMT management: a) Managing the group of roles that can interact with the TSF data.	There is no management function that is applicable for the management items on the left.
FMT_SMF.1	There are no management activities foreseen for this component.	N/A
FMT_SMR.1[1]	The following actions could be considered for the management functions in FMT management: a) Managing the group of users that are part of a role.	There is no management function that is applicable for the management items on the left.
FMT_SMR.1[2]	The following actions could be considered for the management functions in FMT management: a) Managing the group of users that are part of a role.	There is no management function that is applicable for the management items on the left.
FMT_SMR.1[3]	The following actions could be considered for the management functions in FMT management: a) Managing the group of users that are part of a role.	There is no management function that is applicable for the management items on the left.
FMT_SMR.1[4]	The following actions could be considered for the management functions in FMT management: a) Managing the group of users that are part of a role.	There is no management function that is applicable for the management items on the left.

Functional requirement components	Management items listed in CC Part 2	Application
FPT_RVM.1	There are no management activities foreseen.	N/A
FPT_SEP.1	There are no management activities foreseen.	N/A
FTA_SSL.3[1]	The following actions could be considered for the management functions in FMT: a) Specify the time that a user who generates the termination of interaction session to each user is inactive; b) Specify the default time that a user who generates the termination of interaction session is inactive.	***• Modification function of auto reset operational setting data***
FTA_SSL.3[2]	The following actions could be considered for the management functions in FMT: a) Specify the time that a user who generates the termination of interaction session to each user is inactive; b) Specify the default time that a user who generates the termination of interaction session is inactive.	***• Modification function of auto reset operational setting data***

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*]:
General user who creates the box

FMT_SMR.1.2[1]
The TSF shall be able to associate users with roles.
Hierarchical to: No other components
Dependencies: FIA_UID.1 (N/A)

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*]: ***General user who is a valid user of the box***
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*]: ***Administrator***
FMT_SMR.1.2[3]
The TSF shall be able to associate users with roles.

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

FMT_SMR.1[4]	**Security Roles**
FMT_SMR.1.1[4]	
The TSF shall maintain the roles [assignment: the a*uthorised identified roles*].	
[assignment: *the authorised identified roles*]: ***Service engineer***	
FMT_SMR.1.2[4]	
The TSF shall be able to associate users with roles.	
Hierarchical to:	No other components
Dependencies:	FIA_UID.1 (FIA_UID.2[4])

5.1.1.4. Protection of the TSF

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

FPT_SEP.1	**TSF Domain Separation**
FPT_SEP.1.1	
The TSF shall maintain a security domain for its own execution that protects it from	

interference and tampering by untrusted subject.	
FPT_SEP.1.2	
The TSF shall enforce separation between the security domains of subjects in the TSC.	
Hierarchical to:	No other components
Dependencies:	No dependencies

5.1.1.5. TOE Access

FTA_SSL.3[1] TSF-initiated termination	
FTA_SSL.3[1]	
The TSF shall terminate an interactive session after a [assignment: *time interval for user inactivity*]	
[assignment: *time interval for user inactivity*] ***The time set according to Auto Reset Operational Settings Data from last operation during operation of the panel administrator function.***	
Hierarchical to:	No other components
Dependencies:	No dependencies

FTA_SSL.3[2]	**TSF-initiated termination**
FTA_SSL.3[2]	
The TSF shall terminate an interactive session after a [assignment: *time interval for user inactivity*]	
[assignment: *time interval for user inactivity*] ***The time set according to Auto Reset Operational Settings Data form last operation during operation of the PC administrator function.***	
Hierarchical to: No other components	
Dependencies: No dependencies	

5.1.2. Minimum Security Strength of Function

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

5.1.3. TOE Security Assurance Requirements

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

Table 6. TOE Security Assurance Requirements

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

5.2. Security Requirements for the IT environment

The security function requirements required for the IT environment are described. Those regulated in CC Part 2 must be directly used for all the functional requirements components, and the same labels must be used as well. In the following description, when items are indicated in "italic" and "bold" it means that they are assigned or selected. When indicated in "italic" and "bold" and an "underline" it means that they are refined. An identifier "E" in the parentheses, after the label, is used in order to explicitly show this function requirement is a security requirement for the IT environment. In addition, numbers following an "E" such as "…[E1]", "…[E2]" indicate that the corresponding function requirement is repeating. The label in the parentheses "( )"in the dependency section indicates a label for the security function requirements used in this ST. When it is a dependency that is not required to be used in this ST, it is described as "N/A" in the same parentheses.

5.2.1. Security Functional Requirements for the IT Environment

5.2.1.1. Identification and Authentication

FIA_SOS.1[E] Verification of secrets
FIA_SOS.1.1[E]
Printer driver of the client PC shall provide a mechanism to verify that the ***secure print password meets*** [assignment: *Defined quality metric*].
[assignment: *Defined quality metric*]: ***4-digit number (0 to 9)***
Hierarchical to: No other components **Dependencies:** No dependencies

FIA_UAU.7[E] Protected Authentication Feedback
FIA_UAU.7.1[E]
Box utility shall provide only [assignment: *list of feedback*] to the user while the authentication is in process.
[assignment: *list of feedback*]: ***Display "*" for each character of character data entered as a box password or administrator password.***

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

5.2.2. Security assurance requirements for the IT environment

Security assurance requirements for the IT environment are not regulated.

6. TOE Summary Specification

6.1. TOE Security Functions

The security functions of the TOE satisfy, as shown in Tables 7 and 8 below, all of the TOE security function requirements described in the previous chapter.

Table 7. Security Function Name and Identifier for TOE

Identifier	TOE Security Function
F.ADMIN-PANEL	Panel administrator mode security function
F.ADMIN-PC	PC administrator mode security function
F.COPY	Remaining copy job information data security function
F.SECURE-PRINT	Secure print security function
F.SERVICE	Service mode security function
F.BOX-PANEL	Panel box security function
F.BOX-PC	PC box security function
F.BOX-UTILITY-1	Box utility security function
F.BOX-UTILITY-2	Administrator box utility security function

Table 8. Correspondence Between TOE Security Functions and TOE Security Function Requirements

TOE Security Function TOE Security functional requirement	F.ADMIN-PANEL	F.ADM IN-PC	F.COPY	F.SECURE-PRINT	F.SERVICE	F.BOX-PANEL	F.BOX-PC	F.BOX-UTILITY-1	F.B OX-UTILITY-2
FDP_ACC.1[1]				●					
FDP_ACC.1[2]						●	●	●	●
FDP_ACC.1[3]			●						
FDP_ACF.1[1]				●					
FDP_ACF.1[2]						●	●	●	●
FDP_ACF.1[3]			●						

TOE Security Function TOE Security functional requirement	F.ADMIN-PANEL	F.ADM IN-PC	F.COPY	F.SECURE-PRINT	F.SERVICE	F.BOX-PANEL	F.BOX-PC	F.BOX-UTILITY-1	F.B OX-UTILITY-2
FIA_AFL.1[1]				●					
FIA_AFL.1[2]						●	●	●	
FIA_AFL.1[3]	●	●							●
FIA_AFL.1[4]					●				
FIA_SOS.1[1]		●					●		
FIA_SOS.1[2]	●								
FIA_SOS.1[3]					●				
FIA_UAU.2[1]				●					
FIA_UAU.2[2]						●	●	●	
FIA_UAU.2[3]	●	●							●
FIA_UAU.2[4]					●				
FIA_UAU.6	●				●				
FIA_UAU.7	●	●		●	●	●	●	●	●
FIA_UID.2[1]				●					
FIA_UID.2[2]						●	●	●	
FIA_UID.2[3]	●	●							●
FIA_UID.2[4]					●				
FMT_MOF.1	●								
FMT_MSA.1[1]		●					●		
FMT_MSA.1[2]	●	●							
FMT_MSA.3[1]				●					
FMT_MSA.3[2]							●		
FMT_MSA.3[3]			●						
FMT_MTD.1[1]	●	●							
FMT_MTD.1[2]	●								
FMT_MTD.1[3]		●					●		
FMT_MTD.1[4]					●				
FMT_MTD.1[5]					●				

TOE Security Function TOE Security functional requirement	F.ADMIN-PANEL	F.ADM IN-PC	F.COPY	F.SECURE-PRINT	F.SERVICE	F.BOX-PANEL	F.BOX-PC	F.BOX-UTILITY-1	F.B OX-UTILITY-2
FMT_SMF.1	●	●			●		●		
FMT_SMR.1[1]							●		
FMT_SMR.1[2]							●		
FMT_SMR.1[3]	●	●							
FMT_SMR.1[4]					●				
FPT_RVM.1	●	●		●	●	●	●	●	●
FPT_SEP.1	●	●	●	●	●	●	●	●	●
FTA_SSL.3[1]	●								
FTA_SSL.3[2]		●							

6.1.1. F.ADMIN-PANEL (Panel Administrator Mode Security Function)

F.ADMIN-PANEL is a series of security functions for the administration mode that are accessed from the operations panel on the MFP body, such as the administrator identification and authentication functions, the security management function that changes the administrator mode password, the box password, and the box identifier, the operation setting function for the Unauthorized Access Lock Function, the Access Lock Release Function, etc.

<Identification and authentication function during access to the administrator mode>

- Identifies the accessing user as an administrator by requesting access to the administrator mode.

- Provides an administrator mode password authentication mechanism that authenticates the accessing user as the administrator using the 8-digit number administrator mode password in response to the access request to the administrator mode.

- Returns "*" for each character as feedback for the entered administrator mode password.
- Failing at authentication three times makes it determine that an unauthorized access is being carried out and this authentication function is locked (※There is no function for releasing the lock.)

<Security management functions in administrator mode that are accessed from the MFP body operations panel>

- If authentication of the administrator has been carried out for the accessing of the administrator mode from the MFP body operations panel, access and operation are permitted for (1) the administrator mode password change function, (2) the operational settings function of the Unauthorized Access Lock Function, (3) the Access Lock Release Function, (4) the change function for Auto Reset Operational Settings Data, and (5) the settings change function for memory recall settings data.

(1) Administrator mode password change function,

- ➢ Provides an administrator mode password authentication mechanism that re-authenticates that it is the administrator with the administrator mode password.
- ➢ Returns "*" for each character as feedback for the entry of an administrator mode password during re-authentication.
- ➢ Checks that the newly set administrator mode password is an 8-digit number, and when the entry of a newly set box password and the re-entry to prevent entry errors are both received and match, the password is replaced as the administrator mode password.
- ➢ Counts the count value for the detected number of unauthorized accesses to the administrator mode by the erroneous entries of the administrator mode password that are entered for re-authentication. Failing three times cancels the access permission to the administrator mode and locks the authentication function that accesses administrator mode.

(2) Operational settings function of the Unauthorized Access Lock Function

- ➢ Turn on the Unauthorized Access Lock Function by selecting/executing "enable."
- ➢ Turn off the Unauthorized Access Lock Function by selecting/executing "disable."

(3) Access Lock Release Function

- Releases the lock on the authentication function that authenticates a general user who is a valid user of a secure print job by clearing the count value to zero for detected unauthorized accesses to secure print for each secure print job.

- Releases the lock on the authentication function that authenticates a general user who is a valid user of a box, by clearing the count value to zero for detected unauthorized accesses to the box for boxes.

(4) Change function for Auto Reset Operational Settings Data

- Set operation of Auto Reset Function to "No" or within time range 1~9 minutes.

(5) Settings change function for memory recall settings data

- Turn on memory recall settings data by selecting/executing "enable," and make operational the Memory Recall Copy Function (leave in reprint enabled condition, without deleting copy job data files).

- Turn off memory recall settings data by selecting/executing "disable," and stop the Memory Recall Copy Function (automatically delete copy job data files after printing, not leaving them in reprint enabled condition).

<Auto Reset Function for operation in administrator mode for access from the MFP body operations panel>

- Regarding access to the administrator mode from the MFP body operations panel, if an inactive condition exceeds the time specified by the Auto Reset Operational Settings Data after the administrator has been authenticated, the access permitted condition for the administrator mode is cancelled.

- This function operates by the time specified by Auto Reset Operational Settings Data.

6.1.2. F.ADMIN-PC (PC Administrator Mode Security Function)

F.ADMIN-PC is a series of security functions for the administration mode that are accessed from the client PC, such as the administrator identification and authentication functions, the box setting management function that changes the box password and the box identifier, etc.

<Identification and authentication function during access to the administrator mode>

- Identifies the accessing user as an administrator by requesting access to the administrator mode from the client PC.
- Provides an administrator mode password authentication mechanism that authenticates the accessing user as the administrator using the 8-digit number administrator mode password in response to the access request to the administrator mode.
- Returns "*" for each character as feedback for the entered administrator mode password.
- Failing at authentication three times makes it determine that an unauthorized access is being carried out and this authentication function is locked. (※There is no function for releasing the lock.)

<Security management functions in administrator mode that are accessed from the client PC>

- If authentication of the administrator has been carried out for the accessing of the administrator mode from the client PC, access and operation are permitted for functions that change the box identifier and box password for any box: (1) the box settings management function, (2) the change function for Auto Reset Operational Settings Data, and (3) the settings change function for memory recall settings data.

(1) Box settings management function

- ➢ Box identifier change receives input for the box identifier to be newly set and changes the name as box identifier of the corresponding box if a box identifier for and identical name is not registered.
- ➢ Box identifier change receives input of the box password to be newly set and re-input of the password to prevent erroneous input, and then changes the password as the corresponding box password when the input matches.
- ➢ Checks that the box password is 4~64 characters and ASCII code 0x20~0x7E (95 types in English one-byte characters and one byte symbols).

(2) Change function for Auto Reset Operational Settings Data

- ➢ Set operation of Auto Reset Function to "No" or within time range 1~9 minutes.

(3) Settings change function for memory recall settings data

- Turn on memory recall settings data by selecting/executing "enable," and make operational the Memory Recall Copy Function (leave in reprint enabled condition, without deleting copy job data files).

- Turn off memory recall settings data by selecting/executing "disable," and stop the Memory Recall Copy Function (automatically delete copy job data files after printing, not leaving them in reprint enabled condition).

<Auto Reset Function for operation in administrator mode for access from the client PC>

- Regarding access to the administrator mode from the client PC, if an inactive condition exceeds the time specified by the Auto Reset Operational Settings Data after the administrator has been authenticated, the access permitted condition for the administrator mode is cancelled.

- This function operates at 5 minutes when the Auto Reset Operational Settings Data is 1~5 minutes, at 6~9 minutes when the Auto Reset Operational Settings Data is 6~9 minutes, and at 10 minutes when the Auto Reset Operational Settings Data is "No."

6.1.3. F.COPY (Remaining Copy Job Information Data Protection Function)

F.COPY is a function that automatically deletes copy job information data that is scanned image data, after printing by the Copy Function from the MFP body operations panel.

- When the Copy Function is executed, copy job information data that has memory recall settings data "Off" is deleted by the process operating the copy job after printing. (※With when the Memory Recall Copy Function has been set to disable condition by the administrator function, the memory recall settings data having the security attributes for copy job information data file will always be "Off.")

6.1.4. F.SECURE-PRINT (Secure Print Security Function)

F.SECURE-PRINT is an access control function that permits secure print job information data print operations after identifying and authenticating that a user of secure print job information data is valid for access to the secure print job information data from the MFP body operations panel.

<Secure print job registration function>

- Registration of the secure print job information data file is offered to the general user.

- Assigns a uniquely identified job ID to the transmitted secure print data with the secure print password set by the printer driver of the client PC as a secure print job information data file, and registers it.

<Identification and authentication function to print the secure print job>

- When a secure print job in standby status is selected by the MFP body operations panel, it provides a secure print password authentication mechanism that authenticates that the person who accesses the selected secure print job information data is a general user who is a valid user of the secure print job, using a 4-digit secure print password.

- Returns "*" for each character as feedback for the entry of the secure print password.

- When the authentication fails three times, it determines that an unauthorized access is being carried out and it locks the authentication function for accessing the secure print job information data. This locked status is released by executing the Access Lock Release Function for the secure print job provided by F.ADMIN-PANEL.

<Access control function for printing secure print jobs>

- After a general user is authenticated as the valid user of a secure print job information data file, print operation is permitted for a secure print job information data file having a "job ID" that matches the subject attributes corresponding to the process operating the secure print job based on secure print job access control rules.

6.1.5. F.SERVICE (Service Mode Security Function)

F. SERVICE is a series of security functions for service mode that are accessed from the MFP body operations panel, such as the service engineer identification and authentication function, the modification function for the service code, and the initialization function for the administrator mode password.

<Identification and authentication function for access to the service mode>

- Identifies the accessing user as a service engineer by requesting access to the service mode (executes an operations procedure for the service mode that is not disclosed to anyone other than to service engineers).

- When it receives an operations procedure for the service mode, it provides a service code authentication mechanism that authenticates that the accessing user to the service mode is the service engineer by using a password (service code) comprised of 8 digits of numbers, "#" or "*".

- Returns "*" for each character as feedback for the service code entry.

- When the authentication fails three times, it determines that an unauthorized access is being carried out and it locks the authentication function for access to the service mode. (※There is no function for releasing the lock.)

<Security management function for service mode>

- When the person accessing the service mode is authenticated as the service engineer, it permits the access and operation of the security management function for the service mode.

  (1) Modification function of the service code

  - The modification function for the service code provides a service code authentication mechanism that re-authenticates the service engineer, after an additional operation procedure, which is not disclosed, is entered in the service mode.

  - Returns "*" for each character as feedback for the service code entry during the re-authentication.

  - Check that the newly set service code is comprised of 8 digits of numbers, "#" or "* and receive the service code entry for a new setting, and the re-entry to prevent an error, and when both are identical, it replaces the service code with the password.

  - When the service code that was entered for this re-authentication is wrong, it cancels the access permission to the service mode, and increments the count value of detected unauthorized access for the service engineer.

  (2) Initialization function for the administrator mode password

  - When the initialization function for the administrator mode password is executed, it sets the administrator mode password to default at the setup.

6.1.6. F.BOX-PANEL (Panel Box Security Function)

F.BOX-PANEL is an access control function that identifies and authenticates that a general user's access to a box data from the MFP body operations panel is a valid use of the box data, and controls the access to the box.

<Identification and authentication function for accessing a box>

- When a box to be accessed is selected, it provides a box password authentication mechanism that authenticates that the user, who is attempting access, is the general user who is the valid user of the corresponding box with a box password that is comprised of 4 to 64 digits of ASCII code 0x20 to 0x7E (95 types of English one-byte characters and one byte symbols)
- Returns "*" for each character as feedback for the box password entry.
- When the authentication trial fails 3 times, it locks the authentication function for accessing the target box. This locked state is released by executing the Access Lock Release Function for the box provided by F.ADMIN-PANEL.

<Box access control function after identification and authentication>

- When a general user is authenticated as a general user who is a valid user of the box, based on the box access control function, for the process that operates the box, the "read the box data in the box" operation for a box with a "box identifier" that is identical to the subject attributes is permitted. (By permitting reading of box data within this box, the Email transmission operation and FTP transmission operation are permitted from the MFP body operations panel.)

6.1.7. F.BOX-PC (PC Box Security Function)

F.BOX-PC is a security function that identifies and authenticates that a general user's access to a box from a client PC is a valid use of the box data, controls the access to the box, creates a box, and manages the setting of the box.

<Box creation function>

- A box creation function is provided to general users.
- When the box creation function starts up, a process that operates the box starts up.

- When a box identifier entered by a general user through the process to operate the box has not been set to another box, a box with the box identifier entered by the general user as the attribute is created. (If it already exists, it is denied.)

<Identification and authentication function for accessing a box>

- When a box to be accessed is selected, it provides a box password authentication mechanism that authenticates that the user, who is attempting access, is the general user who is the valid user of the box with a box password that is comprised of 4 to 64 digits of ASCII code 0x20 to 0x7E (95 types of English one-byte characters and one byte symbols)
- Returns "*" for each character as feedback for the box password entry.
- When the authentication trial fails 3 times, it locks the authentication function for accessing the target box. This locked state is released by executing the Access Lock Release Function for the box provided by F.ADMIN-PANEL.

<Box access control function after identification and authentication>

- When a general user is authenticated as a general user who is a valid user of the box, based on the box access control function, for the process that operates the box, the "read the box data in the box" operation for a box with a "box identifier" that is identical to the subject attributes is permitted. (By permitting reading of box data within this box, download operations from the client PC become possible.)

<Box setting management function>

- Provides a function to change the settings of a box (modification of the box identifier, modification of the box password) for the concerned box to the identified and authenticated valid user of the box.
- During the modification of the box password, the entry of a new box password to be set and the re-entry to prevent erroneous entries are received, and when both are identical, the box password is modified.
- Checks whether the newly set box password is comprised of 4 to 64 digits of ASCII code 0x20 to 0x7E (95 types of English one-byte characters and one byte symbols).
- When the authentication trials fail 3 times, it locks the authentication function for the general user who is a valid user of the box. This locked state is released by executing the Access Lock Release Function for the box provided by F.ADMIN-PANEL.

6.1.8. F.BOX-UTILITY-1 (Box Utility Security Function)

F.BOX-UTLITY-1 is an access control function that identifies and authenticates a valid general user of box data for access to box data used by a special application from a client PC, and controls access to the box.

<Identification and authentication function for accessing a box>

- When a box to be accessed is selected, it provides a box password authentication mechanism that authenticates that the user, who is attempting access, is the general user who is the valid user of the box with a box password that is comprised of 4 to 64 digits of ASCII code 0x20 to 0x7E (95 types of English one-byte characters and one byte symbols)

- When the authentication trial fails 3 times, it locks the authentication function for accessing the target box. This locked state is released by executing the Access Lock Release Function for the box provided by F.ADMIN-PANEL.

<Box access control function after identification and authentication>

- When a general user is authenticated as a general user who is a valid user of the box, based on the box access control function, for the process that operates the box, the "read the box data in the box" operation for a box with a "box identifier" that is identical to the subject attributes is permitted. (By permitting reading of box data within this box, download operations, preview operations, and thumbnail display operations become possible by using a box utility from the client PC.)

6.1.9. F.BOX-UTILITY-2 (Administrator Box Utility Security Function)

F.BOX-UTILITY-2 is a function that authenticates an administrator accessing a box from the administrator client PC by using a box utility that is a special application.

<Identification and authentication function for box data backup operation and restore operation >

- Provide an administrator mode authentication mechanism that authenticates that the user, who is requesting the backup operation of box data and the restore operation of backed up box data by using the box utility from the client PC, is the administrator with an administrator mode password that is comprised of 8 digits number.

- When the authentication trial fails three times, it determines that an unauthorized access is being carried out and it locks the authentication function. (※There is no function for releasing the lock.)

<Box access control function after authentication (backup operation)>

- If the administrator is verified, the "reading of box data within a box" operation (box data backup operation) for all boxes is permitted in relation to processes operating boxes having an "administrator identifier."

< Box access control function after authentication (restore operation)>>

- If the administrator is verified, the "writing of box data to a box" operation (restore operation for backed up box data) for all boxes is permitted, based on box access control, in relation to processes operating boxes having an "administrator identifier."

6.2. TOE Security Strength of Function

The TOE security functions having probabilistic/permutational mechanisms are the administrator mode password authentication mechanism by F. ADMIN-PANEL, P.ADMIN-PC, F.BOX-UTILITY-2, the secure print password authentication mechanism by F.SECURE-PRINT, the box password authentication mechanism by F.BOX-PANEL, F.BOX-PC, F.BOX-UTILITY-1, and the service code authentication mechanism by F.SERVICE. The strength of each of the functions satisfies the SOF-Basic.

6.3. Assurance Measures

The following table shows the assurance measures to meet the component of the TOE security assurance requirements for EAL3 that are stipulated in Table 9.

Table 9. Correspondence between TOE Assurance Requirements and assurance measures

TOE Security Assurance Requirement		Component	Assurance Measures
Class ACM: Configuration management	CM capabilities	ACM_CAP.3	• Configuration management plan • Configuration list • CM record
	CM scope	ACM_SCP.1	
Class ADO: Delivery and Operation	Delivery	ADO_DEL.1	Delivery instructions
	Installation, generation and start-up	ADO_IGS.1	• Installation checklist (Japanese) • Installation checklist (English) ※The physical installation procedure for the TOE on the market is described in service manual “bizhub C350 Service Manual [Security Functions] (Japanese) and bizhub C350 Service Manual [Security Functions]” (English).
Class ADO: Development	Functional specification	ADV_FSP.1	Security function specifications
	High-level design	ADV_HLD.2	Security high level design specifications
	Representation correspondence	ADV_RCR.1	Representation correspondence analysis report
Class AGD: Guidance Document	Administrator guidance	AGD_ADM.1	• bizhub C350 Users Guide [Security Functions] (Japanese) • bizhub C350 Users Guide [Security Functions] (English) • CF2203 Users Guide[Security Functions](English) • 8802 Users Guide [Security Functions] (English) • bizhub C350 Service Manual [Security Functions] (Japanese) • bizhub C350/CF2203/8022 Service Manual [Security Functions] (English)
	User Guidance	AGD_USR.1	
Class ALC: Life Cycle Support	Development security	ALC_DVS.1	Development security instructions
Class ATE:	Coverage	ATE_COV.2	Coverage analysis report

TOE Security Assurance Requirement		Component	Assurance Measures
Test	Depth	ATE_DPT.1	Depth analysis report
	Functional tests	ATE_FUN.1	Test specification and results report
	Independent testing	ATE_IND.2	MFP control software including TOE
Class AVA: Vulnerability Assessment	Misuse	AVA_MSU.1	Reflected in the guidance documents
	Strength of TOE security functions	AVA_SOF.1	Strength of Function analysis report
	Vulnerability analysis	AVA_VLA.1	Vulnerability analysis report

7. PP Claims

There is no conformance to a PP in this ST.

8. Rationale

The justification of the contents regulated in this ST is described.

8.1. Security Objectives Rationale

8.1.1. Necessity

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

Table 10. Conformity of Security Objectives to assumptions and Threats

Assumption/Threat Security objectives	A.ADMIN	A.AUTH	A.HDD	A.NETWORK	A.PHYICAL	A.SERVICE	A.SETTING	T. ACCESS-SECURE-PRINT	T. ACCESS-BOX	T.ACCESS-COPY-DATA	T.SEND-BOX-DATA	P.BEHAVIOR-FUNCTION
O.ACCESS-ADMIN								●	●	●		●
O.ACCESS-BOX									●			
O. ACCESS-SECURE-PRINT								●				
O.ACCESS-SERVICE								●	●	●	●	●
O.CONTROL-COPY										●		
O.I&A-ADMIN								●	●	●	●	●
O.I&A-SERVICE								●	●	●	●	●
O.I&A-USER								●	●			
OE.FEED-BACK									●			
OE.SECURE-PRINT-QUALITY								●				
OE-N.ADMIN	●											
OE-N.AUTH		●										
OE-N.HDD			●									
OE-N.NETWORK				●								
OE-N.PHYSICAL					●							
OE-N.SERVICE						●						
OE-N.SESSION								●	●	●	●	●
OE-N.SETTING-1							●					

OE-N.SETTING-2										●		

8.1.2. Sufficiency (Assumptions)

The security objectives for the assumptions are described as follows.

- **A.ADMIN (Personnel Conditions to be an Administrator)**

  This condition assumes that administrators are not malicious.
  With OE-N.ADMIN, the organization that uses the MFP assigns personnel who are reliable in the organization that uses the MFP, so the reliability of the administrator is assured.
  Accordingly, this condition is realized.

- **A.AUTH (Operation Condition Regarding Password)**

  This condition assumes that each password (secure print password, box password, administrator mode password, and service code) used for the use of the TOE is not divulged by the user of the password.
  OE-N.AUTH regulates that the person in charge of the organization that uses the MFP enforces compliance, with the operation regulation for administrator password to the administrator.
  This security objective regulates that the administrator enforces compliance with the operation rule, regarding for the secure print password and box password to general users.
  In addition, this security objective regulates that the person in charge of the organization that manages the maintenance of the MFP enforces compliance of the operation rule regarding the service code to the service engineer.
  Therefore, the handling of each password that is used for the use of the TOE is explicitly regulated by the operation rule, and so it is assured that the divulging of a password during the operation should not occur. Accordingly, this condition is realized.

- **A.HDD (Hardware environment condition used by the MFP)**

  This condition assumes that only an HDD having an HDD Lock Function is used with the MFP in which the TOE is loaded, that the set HDD lock password will not be exposed by users, and that assets in the HDD will be protected even if it is removed and/or unauthorized data analysis is attempted.
  OE-N.HDD regulates that service engineers install an HDD having an HDD lock function into the MFP in which the TOE is loaded and that administrators set suitable HDD lock passwords and perform operations management. This assures inability to read data due to the HDD Lock Function, even if unauthorized data analysis is attempted, and assures confidentiality of the protective assets.
  Accordingly, this condition is realized.

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

  This condition assumes that there are no wiretapping activities for the intra-office LAN and no access by an unspecified person from an external network, because of a variety of conditions on the network environment connected to the MFP.
  OE-N.NETWORK regulates measures such as the installation of devices such as a switching hub and encoding between the MFP and client PC, and executes an appropriate environmental setting that does not allow wiretapping, in order to realize a network environment that does not allow wiretapping of the intra-office LAN. It also regulates the installation of devices that block access from external networks to the MFP, and executes an appropriate setting to block external access.
  Accordingly, this condition is realized.

  A network environment that does not allow wiretapping can be realized specifically using the following methods, etc.

  (1) Structure the intra-office LAN using switching hubs only and use an intra-office LAN environment based on the operation policy of an office that prohibits wiretapping activities.

  (2) Connect the MFP to the intra-office LAN via a specific device and execute a setting by which all the communication data between the device and client PCs on the intra-office LAN are encoded by, for example, IPsec.

- **A.PHYSICAL (Installation Conditions for the MFP)**

  This condition assumes that the place where the MFP with the TOE is installed is a physically protected place where only the general users, administrator and service engineer are allowed to enter.
  OE-N.PHYSICAL regulates that the installation of the MFP with the TOE is in an office that is physically protected. In addition, this security objective regulates the execution of an operation management that limits entry to the office to only general users, an administrator and a service engineer, and this assures the physical protection of the TOE.
  Accordingly, this condition is realized.

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

  This condition assumes that service engineers are not malicious.
  With OE-N.SERVICE, the organization that manages the maintenance of the MFP assigns reliable personnel from the organization that manages the maintenance of the MFP as the service engineer, so that the reliability of service engineers is assured.
  Accordingly, this condition is realized.

- **A.SETTING (Security Function Operational Settings Conditions)**

  This condition assumes that the Unauthorized Access Lock Function is always in operation.
  OE-N.SETTING-1 regulates that administrators always operate the Unauthorized Access Lock Function in the use of the MFP in which the TOE is loaded, and assures operation as expected by these security control functions.
  Accordingly this condition is realized.

8.1.3. Sufficiency (Threats)

The security objectives against threats are described as follows.

- **T.ACCESS-SECURE-PRINT (Unauthorized Operation of Secure Print Job Information Data)**

  This threat assumes the possibility that secure print job information data is accessed from the MFP body operations panel, and the secure print job information data is unlawfully printed. To counter this, verification is carried out that the accessing user is a valid user and access and operation by persons other than authorized valid users is limited.

  As a security objective to counter this threat, O.I&A-USER regulates the identification and authentication of whether the user who is accessing the secure print job information data is a general user who is a valid user of the secure print job. In addition, O.ACCESS-SECURE-PRINT regulates that only a general user who is identified and authenticated as a valid user is permitted to execute the print operation for secure print job information data, which is the target of the access.

  With this authentication function, in order to maintain the strength of function, a certain length of password is required. OE.SECURE-PRINT-QUALITY regulates such that only data, which satisfies the quality metric that is regulated as a secure print password that is configured for a secure print for the printer driver that is installed in the client PC, is received.

  In addition, an operation setting function for the Unauthorized Access Lock Function that detects unauthorized access during the authentication function of a general user, who is a valid user of a secure print job, and an Access Lock Release Function that releases the lock status of the authentication function, are provided in administrator mode. But, O.I&A-ADMIN regulates the identification and authentication of whether the user who is accessing the administrator mode is actually the administrator, and in addition, O.ACCESS-ADMIN regulates it so that only the administrator is allowed to operate the administrator function. OE-N.SESSION regulates the operation terminating the session after terminated use of the administrator function. Through the above, we are protected from unauthorized access to the security management function related to the secure print job information data in the administrator mode,

Furthermore, as countermeasures against service mode, which has a managing function to initialize the administrator mode password, O.I&A-SERVICE regulates the identification and authentication of whether the user who is accessing the service mode is actually the service engineer, and O.ACCESS-SERVICE regulates so that only the service engineer is allowed to operate the security related functions in service mode, and operation terminating that session after terminated use of the security management function for the service mode is regulated by OE-N.SESSION.

Accordingly, fulfillment of these security objectives can sufficiently counter this threat.

- **T.ACCESS-BOX (Unauthorized Operation of Box Data)**

This threat assumes the possibility that the box data is accessed from the client PC and the box data is unlawfully downloaded. To counter this, an accessing user should be verified as a valid user and access and operation by anyone other than a person who is authorized as a valid user should be limited.

As a security objective to counter this threat, O.I&A-USER regulates the identification and authentication of whether the person who is accessing the box is a general user who is a valid user of the box. In addition, O.ACCESS-BOX regulates the permission for the download operation of the box data from the box, which is the target of access, to only be by the identified and authenticated general user who is a valid user. Furthermore, OE-N.SESSION regulates that administrators always execute operations terminating the session after terminated use of the Box Function for general users, and reduces the possibility of unauthorized access.
When it is the access using the box utility, OE.FEED-BACK regulates the returning of the protected appropriate feedback for administrator mode password that is inputted at the time of access.
O.I&A-ADMIN regulates the authentication of whether a user who requests backup and restore operation of box data that is one of the administrator functions, is definitely the administrator. Furthermore, O.ACCESS-ADMIN regulates so that only the administrator is allowed to operate administrator function such as backup operation and restore operation of box data (downloading, uploading operation). In this case, OE.FEED-BACK also regulates the returning of the protected appropriate feedback for the administrator mode password that is input at the time of access.

The operational settings function for the Unauthorized Access Lock Function that detects unauthorized access during the authentication function of a general user who is a valid user of the box, and the Access Lock Release Function that releases the locked state of the concerned authentication function, and the settings management function of the box are administrator functions provided by the administrator mode, and O.I&A-ADMIN regulates the identification and authentication of whether a person who is accessing the administrator mode is actually an administrator, as it does for box data backup operations and restore operations. Furthermore, O.ACCESS-ADMIN regulates so that only administrators are allowed to operate the administrator functions, and OE-N.SESSION regulates operations terminating the session after terminated use of the administrator functions. These methods protect against unauthorized access to the security management function for the box data in the administrator mode.

Moreover, as a countermeasure against the service mode having a management function that initializes the administrator mode password, O.I&A-SERVICE regulates the identification and authentication of whether the person who is accessing the service mode is actually a service engineer. O.ACCESS-SERVICE regulates so that only service engineers are allowed to operate security-related functions in the service mode, and OE-N.SESSION regulates operations terminating the session after terminated use of security management functions in the service mode.

Accordingly, by satisfying these security objectives, it is possible to sufficiently counter these threats.

- **T.ACCESS-COPY-DATA (Unauthorized Operation to Remaining Copy Job Information Data)**

This threat assumes the possibility that the data file of copy job information data enabled for reprinting after normal use could be accessed and exposed. To counter this, when copying documents and materials with high confidentiality, it is necessary to automatically delete the data after printing and realize a condition in which the data cannot be reused.

As a security objective to counter this threat, O.CONTROL-COPY regulates the deleting of scanned copy job information data after printing, and OE-N.SETTING-2 assures security for copy job information data having a possibility of remaining in useable form for use by the Copy Function by regulating to enact settings that do not allow an administrator to use the Memory Recall Copy Function.

The operational function for the Memory Recall Copy Function is offered for the administrator mode, but O.I&A-ADMIN regulates the identification and authentication of whether a person who is accessing the administrator mode is actually an administrator. Furthermore, O.ACCESS-ADMIN regulates so that only administrators are allowed to operate the administrator functions, and OE-N.SESSION regulates operations terminating the session after terminated use of the administrator functions. These methods protect against unauthorized access to the security management function for the box data in the administrator mode.

Moreover, as a countermeasure against the service mode having a management function that initializes the administrator mode password, O.I&A-SERVICE regulates the identification and authentication of whether the person who is accessing the service mode is actually a service engineer. O.ACCESS-SERVICE regulates so that only service engineers are allowed to operate security-related functions in the service mode, and OE-N.SESSION regulates operations terminating the session after terminated use of security management functions in the service mode.

Accordingly, by satisfying these security objectives, it is possible to sufficiently counter these threats.

- **T.SEND-BOX-DATA (Transmission of box data to an Address Not Assumed)**

  This threat assumes the possibility that box data can be transmitted to an address not desired by the user through modification of SMTP server or FTP server settings data registered in the MFP as required address data for E-mail transmission or FTP transmission of box data capable of being operated from the MFP body operations panel. To counter this, it is necessary to restrict users who can access SMTP server and FTP server settings data used for transmission only to authorized users.

  As a security objective to counter this threat, O.I&A-ADMIN regulates the identification and authentication of whether the user who is accessing the administrator functions offering SMTP server and FTP server settings data management functions is actually an administrator. Only authorized administrators are able to operate settings data management functions for the SMTP server and FTP server. Furthermore, OE-N.SESSION regulates operations terminating the session after terminated use of the administrator functions.

  Moreover, as a countermeasure against the service mode having a management function that initializes the administrator mode password, O.I&A-SERVICE regulates the identification and authentication of whether the person who is accessing the service mode is definitely a service engineer. O.ACCESS-SERVICE regulates so that only service engineers are allowed to operate security-related functions in the service mode, and OE-N.SESSION regulates operations terminating the session after terminated use of security management functions in the service mode.

Accordingly, by satisfying these security objectives, it is possible to sufficiently counter these threats.

8.1.4. Sufficiency of Organizational Security Policies

The security objective that includes the measures for organizational security policy is described as follows.

- **P.BEHAVIOR-FUNCTION (Operational Settings Function of Security Functions)**

  The organizational security policy regulates deactivate the Unauthorized Access Lock Function and operational state for the Memory Recall Copy Function (no operation at memory recall off copy) in order to design convenience of operation for cases of use in a secure environment. In order to realize this, it is necessary to provide an operational settings function for each function. In addition, because the functions have a large impact on the security configuration, management of each operational settings function must be restricted to trustworthy personnel.

  The security objective that realizes the organizational security policy is regulated by O.I&A-ADMIN for the identification and authentication of whether the person accessing the administrator mode is actually an administrator. In addition, it is regulated by O.ACCESS-ADMIN to permit only administrators operate the administrator functions, and it is regulated by OE-N.SESSION operations terminating the session after terminated use of the administrator functions.

  Moreover, as a countermeasure against the service mode having a management function that initializes the administrator mode password, O.I&A-SERVICE regulates the identification and authentication of whether the person who is accessing the service mode is actually a service engineer. O.ACCESS-SERVICE regulates so that only service engineers are allowed to operate security-related functions in the service mode, and OE-N.SESSION regulates operations terminating the session after terminated use of security management functions in the service mode.

  Accordingly, by fulfilling these two security objectives, it sufficiently realizes the organizational security policy.

8.2. IT Security Requirements Rationale

8.2.1. Rationale for IT Security Functional Requirements

8.2.1.1. Necessity

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

Table 11. Conformity of IT Security Functional Requirements to Security Objectives

Security Objective Security Functional Requirement	O.ACESS-ADMIN	O.ACESS-SECURE-PRINT	O.ACCESS-BOX	O.ACCESS-SERVICE	O.CONTROL-COPY	O.I&A-ADMIN	O.I&A-SERVICE	O.I&A-USER	OE.FEED-BACK	OE.SECURE-PRINT-QUALITY
FDP_ACC.1[1]		●								
FDP_ACC.1[2]			●							
FDP_ACC.1[3]					●					
FDP_ACF.1[1]		●								
FDP_ACF.1[2]			●							
FDP_ACF.1[3]					●					
FIA_AFL.1[1]								●		
FIA_AFL.1[2]								●		
FIA_AFL.1[3]						●				
FIA_AFL.1[4]							●			
FIA_SOS.1[1]								●		
FIA_SOS.1[2]						●				
FIA_SOS.1[3]							●			
FIA_UAU.2[1]								●		
FIA_UAU.2[2]								●		
FIA_UAU.2[3]						●				
FIA_UAU.2[4]							●			
FIA_UAU.6	●		●							
FIA_UAU.7						●	●	●		
FIA_UID.2[1]								●		
FIA_UID.2[2]								●		
FIA_UID.2[3]						●				
FIA_UID.2[4]							●			
FMT_MOF.1	●									

Security Objective Security Functional Requirement	O.ACESS-ADMIN	O.ACESS-SECURE-PRINT	O.ACCESS-BOX	O.ACCESS-SERVICE	O.CONTROL-COPY	O.I&A-ADMIN	O.I&A-SERVICE	O.I&A-USER	OE.FEED-BACK	OE.SECURE-PRINT-QUALITY
FMT_MSA.1[1]	●		●					●		
FMT_MSA.1[2]	●									
FMT_MSA.3[1]		●								
FMT_MSA.3[2]			●					●		
FMT_MSA.3[3]					●					
FMT_MTD.1[1]	●									
FMT_MTD.1[2]	●									
FMT_MTD.1[3]	●							●		
FMT_MTD.1[4]				●						
FMT_MTD.1[5]				●						
FMT_SMF.1	●		●	●				●		
FMT_SMR.1[1]			●					●		
FMT_SMR.1[2]			●					●		
FMT_SMR.1[3]	●									
FMT_SMR.1[4]				●						
FPT_RVM.1	*	*	*	*		*	*	*		
FPT_SEP.1	*	*	*	*	*	*	*	*		
FTA_SSL.3[1]	●									
FTA_SSL.3[2]	●									
FIA_SOS.1[E]										●
FIA_UAU.7[E]									●	

** FPT_RVM.1 and FPT_SEP.1 are the requirements that do not directly relate to the security objectives; however, they are applied as requirements that support functional requirements applied by the associated security objectives as indicated with "*" in the above table. This relationship of support (mutual support) will be described in detail in a later section.*

8.2.1.2. Sufficiency

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

- **O.ACCESS-ADMIN (Management Function Operated by the Administrator)**

  The security objective regulates access to the management functions provided in the administrator mode, and the subjects and operational objectives that operate administrator functions shall be regulated. For this, the following functional requirements are applied.

<Administrator functions for TSF data>

The Unauthorized Access Lock Function restricts to administrator operational settings management by FMT_MOF.1.

The operation of changing an administrator mode password restricts to administrators settings modification operations by FMT_MTD.1[1], FMT_SMF.1. The operation changing an administrator mode password is an important operation in security management, therefore FIA_UAU.6 re-authenticates that it is an administrator upon use.

The modification operation for memory recall settings data restricts to administrators default value change and query operations by FMT_MSA.1[2] and FMT_SMF.1.

The change operation for auto reset settings data restricts to administrators settings change operations by FMT_MTD.1[1] and FMT_SMF.1.

The count value for detected unauthorized access to the box and the count value for detected unauthorized access to a secure print restrict to administrators performance of clear operations by FMT_MTD.1[2] and FMT_SMF.1.

Operations enabling change of box identifiers is added to a general user who is a valid user of the box and to administrators by FMT_MSA.1[1] and FMT_SMF.1.

Operations enabling change of box passwords is added to a general user who is a valid user of the box and to administrators by FMT_MTD.1[3] and FMT_SMF.1.

The role that is allowed by FMT_SMR.1[3] to operate the above-mentioned security management function is the administrator.

<Access time limit of administrator functions>

When an non-operation condition continues and exceeds the defined auto reset setting data during access to administrator functions, permitted access to administrator functions is interrupted by FTA_SSL.3[1] and FTA_SSL.3[2]. (In most cases, usage restrictions for administrator functions are even stricter in order to restrict access even if neglected during use of administrator functions.)

By combining these multiple functional requirements, this security objective is realized.

- **O.ACCESS-SECURE-PRINT (Secure Print Job Access Control)**

This security objective regulates the control of print operations for secure print job information data. Executing the control secure print job creation times and access control for secure print jobs of general users are necessary. The following functional requirements are applied for this objective.

When a registration request for a secure print job is received, a “newly assigned job ID” is created by the process operating secure print jobs by FDP_ACC.1[1] and FDP_ACF.1[1], and access control registering the secure print job information data file with these attributes is executed. In addition, when a “job ID of a secure print job selected by a general user” is received by the process operating secure print jobs by the same functional requirements, access control printing the secure print job information data having the “job ID” is executed.

Basically, the security objective is satisfied by FDP_ACC.1[1], FDP_ACF.1[1] mentioned above. The following described functional requirements are functional requirements related to secure print job access control.

> The default value for a job ID utilized as a security attribute is classified as another job by FMT_MSA.3[1], and a uniquely identified value is assigned.

By combining these multiple functional requirements, this security objective is realized.

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

This security objective regulates the download operation of the box data by a general user. A regulation that controls the creation of a box and access to the box by general users is necessary. The following functional requirements are employed for this.

In accordance with FDP_ACC.1[2] and FDP_ACF.1[2], which define the access control policy to the box, during the process of box operation if there is no box with the same name as the entered “box identifier” in existence, access control is carried out so that an operation to create a box with the name as its attribute is permitted. (If a box with the same name as the entered “box identifier” exists, the operation of creation is denied.)

In addition, with the same functional requirement, access control that permits an operation, to “read the box data in the box” for the box having the “box identifier,” which matches the selected “box identifier” by the general user who is kept by the box operated process, is executed.

With the same functional requirements, the process operating a box having an “administrator identifier” executes access control permitting “reading of box data within a box” operations for all boxes.
Furthermore, “writing of box data within a box” operations for all boxes are permitted.

In principle, this security objective is satisfied by the above-mentioned FDP_ACC.1[2] and FDP_ACF.1[2]. The following functional requirements that are described are the functional requirements related to box access control.

FMT_MSA.3[2] gives a blank (null), which is a permitted value, as the default value of the box identifier that is used as a security attributes. This value can be set to an appropriate default value by only the general user who creates the box.
The role is given by FMT_SMR.1[1] to the general users who create the box, in order to set the blank of the above-described box identifier to an appropriate default value.

FMT_MSA.1[1] and FMT_SMF.1 allow general users who are valid users of the box to change the box identifier.

The role is given by FMT_SMR.1[2] to the general users who are valid users of the box so that they are allowed to operate the above-described security management function.

In addition to the above-mentioned functional requirements that regulate access control, the functional requirements that equivalent to the management of the access control are combined and therefore this security objective is realized.

- **O.ACCESS-SERVICE (Management Function Operated by Service Engineers)**

This security objective regulates the access to the management function for the service engineer that is provided under the service mode. Additionally, the subject that allows operation of each security management function shall be regulated. For this, the following functional requirements are applied.

FMT_MTD.1[4] and FMT_SMT.1 limit the changing of the service code so that only the service engineer can change the setting. The changing of the service code is an important operation for the security management and therefore, FIA_UAU.6 re-authenticates that the person is a service engineer upon use.

The operation to initialize the administrator mode password is limited to the service engineer only by FMT_MTD.1[5] and FMT_SMF.1.

The role is given by FMT_SMR.1[4] to the service engineer so that they can operate the above-mentioned security management functions.

By combining these multiple functional requirements, this security objective is realized.

- **O.CONTROL-COPY (Operational Control of Copy Function)**

This security objective regulates the deleting of copy job information data after it has been printed by use of the Copy Function so that it cannot be reprinted, and it is necessary for control of the delete operation after copy job printing. The following functional requirements are employed for this.

The process operating the copy job executes access control performing the delete operation after printing is completed by FDP_ACC.1[3] and FDP_ACF.1[3] for the copy job information data file that “memory recall settings data” is “Off”.

Basically, this security objective is satisfied by copy job access control that is realized byFDP_ACC.1[3] and FDP_ACF.1[3] requirements described above. The following functional requirements supporting this security objective that are described are the functional requirements related to management primarily needed to fulfill the functional requirements contributing to copy job access control or the functional requirements regulating copy job access control.

The attribute “ memory recall settings data ” used in copy job access control is assigned by FMT_MSA.3[3] at default value “ Off ” corresponding to controlling characteristics not allowing Memory Recall Copy. (A role assigning a substitute default value for overwriting this value doesn’t exist.)

In addition to the above-mentioned functional requirements that regulate copy job access control, the functional requirements that are equivalent to the management of the access control are combined and therefore, this security objective is realized.

- **O.I&A-ADMIN (Identification and Authentication of Administrators)**

This security objective regulates the authentication of whether the person who is accessing the administrator mode is actually the administrator, and appropriate conditions upon authentication are required. The following functional requirements are applied for this.

The user who accesses the administrator mode is identified and authenticated as the administrator by FIA_UID.2[3] and FIA_UAU.2[3]. During the authentication, FIA_UAU.7 returns "*" for each character entered as feedback for the entered administrator mode password. In addition, compliance with the 8 digit number requirement for the administrator mode password being used for authentication is assured by FIA_SOS.1[2].

During accessing of the administrator mode, if the administrator authentication is unsuccessful three times, FIA_AFL.1[3] determines it as an unauthorized access, and it locks the access to the authentication function from thereon, and therefore it is strictly protected.

By combining these multiple functional requirements, this security objective is realized.

- **O.I&A-SERVICE (Identification and Authentication of Service Engineers)**

  This security objective regulates the authentication of whether the person who is accessing the service mode is actually the service engineer, and appropriate conditions upon authentication are required. For this, the following functional requirements are applied.

  The user who accesses the service mode is identified and authenticated as the service engineer by FIA_UID.2[4] and FIA_UAU.2[4]. During the authentication, FIA_UAU.7 returns "*" for each character entered as feedback for the entered service code. In addition, compliance with the 8 digit number, "#" and "*" requirement for the service code being used for authentication is assured by FIA_SOS.1[3].

  During accessing of the service mode, if the service engineer authentication is unsuccessful three times, FIA_AFL.1[4] determines it as an unauthorized access, and it locks the access to the authentication function from thereon, and therefore it is strictly protected.

  By combining these multiple functional requirements, this security objective is realized.

- **O.I&A-USER (Identification and Authentication of General Users)**

This security objective regulates the identification and authentication of whether the user who is accessing a secure print job is a general user who is a valid user of the secure print job. In addition, it also regulates the identification and authentication of whether the user who is downloading the box data is a general user who is a valid user of the box, and therefore, appropriate conditions for the identification and authentication are required. For this, the following functional requirements are applied.

<Identification and authentication of the general user for accessing a secure print job>

FIA_UID.2[1] and FIA_UAU.2[1] identify and authenticate whether a general user is the valid user of the secure print job. (The authentication strength of the secure print password used during this authentication is assured by OE.SECURE-PRINT-QUALITY. See the description in a later section.)

During the authentication of a general user who is the valid user of the secure print job, FIA-UAU.7 returns "*" for each character entered as feedback for the entered secure print password.

If authentication for the secure print job fails 3 times, FIA_AFL.1[1] determines that it is unauthorized access and the authentication function for the general user who is the valid user of the secure print job is locked from that point. The lock can be released by FMT_MTD.1[2] and FMT_SMF.1 related to O.ACCESS-ADMIN.

<Identification and authentication of the general user for accessing the box data>

FIA_UID.2[2] and FIA_UAU.2[2] identify and authenticate whether a person accessing the box is the general user who is a valid user of the box.

The above-mentioned, during each authentication according to FIA_UAU.2[2], FIA_UAU.7 returns "*" for each character entered as feedback for the entered box password.

In addition, FIA_SOS.1[1] assures that the box password being used for the authentication satisfies the quality of 4 to64 English one-byte characters and one-byte symbols.

If any authentication fails 3 times, FIA_AFL.1[2] determines that it is an unauthorized access and the authentication function for the general user who is the valid user of the box is locked from thereon.

The lock can be released by FMT_MTD.1[2] and FMT_SMF.1 related to O.ACCESS-ADMIN.

FMT_MSA.3[2] gives a blank (null), which is a permitted value, as the default value of the box identifier that is used to identify the general user who is a valid user of the box. This value can be set to an appropriate default value by only the general user who creates the box.

The role is given by FMT_SMR.1[1] to the general user who creates the box, in order to set the blank of the above-described box identifier to an appropriate default.

FMT_MSA.1[1] and FMT_SMF.1 allow general users who are valid users of the box, as well as the administrator to change the box identifier.

FMT_MTD.1[3] and FMT_SMF.1 allow general users who are valid users of the box, as well as the administrator to change the box password.

The role is given by FMT_SMR.1[2] to the general users who are valid users of the box, in order to operate the above-mentioned security management function.

By combining these multiple function requirements, this security objective is realized.

- **OE.FEED-BACK (Password Feedback)**

This security objective regulates providing to the user a suitable feedback for input of the box password or administrator mode password in the box utility on a client PC. The following functional requirement is applied for this.

FIA_UAU.7[E] returns “*” as input feedback for a box password or administrator mode password in the box utility of the client PC.

This security objective is realized by this functional requirement.

- **OE.SECURE-PRINT-QUALITY (Quality Metric of Secure Print Password)**

This security objective regulates the addition of a password with an assured strength to the secure print job information data when spooling the secure print to the MFP where the TOE is loaded, at the printer driver of the client PC that is an IT environment.

For this, in accordance with FIA_SOS.1[E], the printer driver of the client PC verifies whether the set secure print password is a 4-digit number. Therefore when the secure print is spooled to the MFP, a 4-digit password is always assigned.

This security objective is realized by this functional requirement.

8.2.1.3. Mutual Support

(1) Complementarity

The IT Security functional requirements for effectively operating other security functional requirements without having a direct corresponding relationship with the security objectives are shown in the following table.

Table 12. Mutual Support Correlations of IT Security Functional Requirements

N/A: Not Applicable

IT Security Functional Requirement	Functional requirement component that operates other security functional requirements validly			
	(1) Bypass Prevention	(2) Interference/Destruction Prevention	(3) Deactivation Prevention	(4) Disabling Detection
FDP_ACC.1[1]	N/A	FPT_SEP.1	N/A	N/A
FDP_ACC.1[2]	N/A	FPT_SEP.1	N/A	N/A
FDP_ACC.1[3]	N/A	FPT_SEP.1	N/A	N/A
FDP_ACF.1[1]	N/A	FPT_SEP.1	N/A	N/A
FDP_ACF.1[2]	N/A	FPT_SEP.1	N/A	N/A
FDP_ACF.1[3]	N/A	FPT_SEP.1	N/A	N/A
FIA_AFL.1[1]	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1	N/A
FIA_AFL.1[2]	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1	N/A
FIA_AFL.1[3]	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1	N/A
FIA_AFL.1[4]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_SOS.1[1]	N/A	FPT_SEP.1	N/A	N/A
FIA_SOS.1[2]	N/A	FPT_SEP.1	N/A	N/A
FIA_SOS.1[3]	N/A	FPT_SEP.1	N/A	N/A
FIA_UAU.2[1]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UAU.2[2]	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1	N/A
FIA_UAU.2[3]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UAU.2[4]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UAU.6	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UAU.7	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UID.2[1]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UID.2[2]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UID.2[3]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FIA_UID.2[4]	FPT_RVM.1	FPT_SEP.1	N/A	N/A
FMT_MOF.1	N/A	FPT_SEP.1	N/A	N/A

IT Security Functional Requirement	Functional requirement component that operates other security functional requirements validly			
	(1) Bypass Prevention	**(2) Interference/Destruction Prevention**	**(3) Deactivation Prevention**	**(4) Disabling Detection**
FMT_MSA.1[1]	N/A	FPT_SEP.1	N/A	N/A
FMT_MSA.1[2]	N/A	FPT_SEP.1	N/A	N/A
FMT_MSA.3[1]	N/A	FPT_SEP.1	N/A	N/A
FMT_MSA.3[2]	N/A	FPT_SEP.1	N/A	N/A
FMT_MSA.3[3]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[1]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[2]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[3]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[4]	N/A	FPT_SEP.1	N/A	N/A
FMT_MTD.1[5]	N/A	FPT_SEP.1	N/A	N/A
FMT_SMF.1	N/A	FPT_SEP.1	N/A	N/A
FMT_SMR.1[1]	N/A	FPT_SEP.1	N/A	N/A
FMT_SMR.1[2]	N/A	FPT_SEP.1	N/A	N/A
FMT_SMR.1[3]	N/A	FPT_SEP.1	N/A	N/A
FMT_SMR.1[4]	N/A	FPT_SEP.1	N/A	N/A
FPT_RVM.1	N/A	FPT_SEP.1	N/A	N/A
FTP_SEP.1	N/A	N/A	N/A	N/A
FTA_SSL.3[1]	N/A	FPT_SEP.1	N/A	N/A
FTA_SSL.3[2]	N/A	FPT_SEP.1	N/A	N/A
FIA_SOS.1[E]	N/A	N/A	N/A	N/A
FIA_UAU.7[E]	N/A	N/A	N/A	N/A

1) Bypass Prevention

TSP execution functions are as follows.

- An identification and authentication function for accessing a secure print job, which is a function that should be executed before permitting the operation advancement of the access control function for the secure print job (executed by FIA_UID.2[1], FIA_UAU.2[1], FIA_UAU.7, and FIA_AFL.1[1]).

- An authentication function for a general user who is a valid user of the box, which is a function that should be executed before permitting the operation advancement of the access control function for the box data and the setting management of the box (change in box password and box identifier) operated by a general user (executed by FIA_UID.2[2], FIA_UAU.2[2], FIA_UAU.7 and FIA_AFL.1[2]).

- An identification and authentication for the administrator, which is a function that should be executed before permitting the operation advancement of the security management function in the administrator mode and access control function for the box data. (Executed by FIA_UID.2[3], FIA_UAU.2[3], FIA_UAU.7 and FIA_AFL.1[3].)

- An administrator re-authentication function, which is a function that should be executed before permitting the operation advancement of the function to change the administrator mode password, from among the security management functions in the administrator mode (executed by FIA_UAU.2[3], FIA_UAU.6, FIA_UAU.7, and FIA_AFL.1[3]).

- A function that identifies and authenticates the service engineer, which is a function that should be executed before permitting the operation advancement of the security management function in the service mode. (executed by FIA_UID.2[4], FIA_UAU.2[4], FIA_UAU.7, and FIA_AFL.1[4]).

- A service engineer re-authentication function, which is a function that should be executed before permitting the operation advancement of the function to change the service code, from among the security management functions in the service mode (executed by FIA_UAU.2[4], FIA_UAU.6, FIA_UAU.7 and FIA_AFL.1[4]).

As described above, the TSP execution function is supported such that everything is always called by FPT_RVM.1 and succeeds.

2) Interference and Destruction Prevention

The TOE offers the following to realize FPT_SEP.1:

- Security domain for secure print job access control processing
- Security domain of box
- Security domain for copy job access control processing
- Security domain in administrator mode
- Security domain in service mode

Accordingly, there is support such that there is no interference or tampering by an unreliable subject of security domain that is the protected asset scope of the TOE and the operational scope of the TSF.

3) Deactivation Prevention

The following operation managements of the functional requirements are restricted by FMT_MOF.1 to administrators, and they offer protection against attacks aiming for deactivation.

- Detection and lock of frequency of unsuccessful authentication (FIA_AFL.1[1], FIA_AFL.1[2], FIA_AFL.1[3]) and authentication for accessing a box (FIA_UAU.2[2]).

4) Disabling Detection

Because of the security functional requirements that have already been employed by taking bypass prevention and interference and destruction prevention into account, even though security that relates to disabling detection is not considered, it has a structure that adequately satisfies the required security objective. Therefore, security functional requirements to detect an attack that disables the security function are not applied.

(2) Dependencies of the IT Security Functional Requirements

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

Table 13. Dependencies of IT Security Functional Requirements

N/A: Not Applicable

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FDP_ACC.1[1]	FDP_ACF.1	FDP_ACF.1[1]
FDP_ACC.1[2]	FDP_ACF.1	FDP_ACF.1[2]
FDP_ACC.1[3]	FDP_ACF.1	FDP_ACF.1[3]
FDP_ACF.1[1]	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1[1], FMT_MSA.3[1]
FDP_ACF.1[2]	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1[2], FMT_MSA.3[2]
FDP_ACF.1[3]	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1[3], FMT_MSA.3[3]
FIA_AFL.1[1]	FIA_UAU.1	FIA_UAU.2[1] <Supplement> FIA_UAU.2 is hierarchical component to FIA_UAU.1 and therefore, the dependencies

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
		are satisfied.
FIA_AFL.1[2]	FIA_UAU.1	FIA_UAU.2[2] <Supplement> FIA_UAU.2 is hierarchical component to FIA_UAU.1 and therefore, the dependencies are satisfied.
FIA_AFL.1[3]	FIA_UAU.1	FIA_UAU.2[3] <Supplement> FIA_UAU.2 is hierarchical component to FIA_UAU.1 and therefore, the dependencies are satisfied.
FIA_AFL.1[4]	FIA_UAU.1	FIA_UAU.2[4] <Supplement> FIA_UAU.2 is hierarchical component to FIA_UAU.1 and therefore, the dependencies are satisfied.
FIA_SOS.1[1]	None	N/A
FIA_SOS.1[2]	None	N/A
FIA_SOS.1[3]	None	N/A
FIA_UAU.2[1]	FIA_UID.1	FIA_UID.2[1] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FIA_UAU.2[2]	FIA_UID.1	FIA_UID.2[2] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FIA_UAU.2[3]	FIA_UID.1	FIA_UID.2[3] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FIA_UAU.2[4]	FIA_UID.1	FIA_UID.2[4] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
		satisfied.
FIA_UAU.6	None	N/A
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2[1], FIA_UAU.2[2], FIA_UAU.2[3], FIA_UAU.2[4]
FIA_UID.2[1]	None	N/A
FIA_UID.2[2]	None	N/A
FIA_UID.2[3]	None	N/A
FIA_UID.2[4]	None	N/A
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[3]
FMT_MSA.1[1]	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	FDP_ACC.1[2], FMT_SMF.1, FMT_SMR.1[2], FMT_SMR.1[3]
FMT_MSA.1[2]	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	FDP_ACC.1[3], FMT_SMF.1, FMT_SMR.1[3]
FMT_MSA.3[1]	FMT_MSA.1 FMT_SMR.1	None. <Reason not fulfilling (1)FMT_MSA.1, (2) FMT_SMR.1> (1) The job ID is an identifier assigned to differentiate from other jobs, and there is no necessity for the capability to operate change of default values or deletion. In addition, there is no necessity to limit users performing query operations because there is no ability for confidentiality in the job ID. (2) The job ID is an identifier assigned to differentiate from other jobs, and there is no necessity to regulate roles specified by default values because there is no necessity to change substitution default values.
FMT_MSA.3[2]	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1[1], FMT_SMR.1[1]
FMT_MSA.3[3]	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1[2] < Reason not fulfilling FMT_SMR.1> The memory recall settings data is managed by

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
		the administrator, and there is no necessity to change security attribute default values of the object created with use of the Copy Function.
FMT_MTD.1[1]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[3]
FMT_MTD.1[2]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[3]
FMT_MTD.1[3]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[2], FMT_SMR.1[3]
FMT_MTD.1[4]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[4]
FMT_MTD.1[5]	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1, FMT_SMR.1[4]
FMT_SMF.1	None	N/A
FMT_SMR.1[1]	FIA_UID.1	None <Reason not fulfilling FIA_UID.1> Box creation is allowed for an arbitrary general user and therefore there is no need to identify the user that is related to this role.
FMT_SMR.1[2]	FIA_UID.1	FIA_UID.2[3] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FMT_SMR.1[3]	FIA_UID.1	FIA_UID.2[3] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FMT_SMR.1[4]	FIA_UID.1	A_UID.2[4] <Supplement> FIA_UID.2 is hierarchical component to FIA_UID.1 and therefore, the dependencies are satisfied.
FPT_RVM.1	None	N/A
FPT_SEP.1	None	N/A
FTA_SSL.3[1]	None	N/A
FTA_SSL.3[2]	None	N/A

Functional Requirements Component for this ST	Dependencies on CC Part 2	Dependencies Relation in this ST
FIA_SOS.1[E]	None	N/A
FIA_UAU.7[E]	FIA_UAU.1	FIA_UAU.2[2], FIA_UAU.2[3]

As described above, sets of IT security requirements have a structure that mutually support each other as a whole, as shown in the dependencies of the (1) complementarity and (2) IT security functional requirements.

8.2.2. Rationale for Minimum Strength of Function

The MFP that is loaded with this TOE is installed in a general office environment where an entry to the office is controlled, and is connected to an intra-office LAN with appropriately controlled connections with external networks. Therefore, there is no possibility that it is directly attacked by unspecified people via the Internet. As long as it has a strength level that can counter the threat by general users who are users of the TOE and a person in the office as an agent, it is acceptable, as explicitly described in section 3.2. Therefore, this TOE regulates security objectives by assuming an unskilled attacker and thus, the selection of the SOF-Basic as the minimum strength of function is reasonable.

8.2.3. Rationale for IT Security Assurance Requirements

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

8.3. Rationale for TOE Summary Specifications

8.3.1. Rationale for the TOE Security Functions

8.3.1.1. Necessity

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

Table 14. Conformity of TOE Security Functions to TOE Security Functional Requirements

TOE Security Function TOE Security Functional Requirement	F.ADMIN-PANEL	F.ADMIN-PC	F.COPY	F.SECURE-PRINT	F.SERVICE	F.BOX-PANEL	F.BOX-PC	F.BOX-UTILITY-1	F.BOX-UTILITY-2
FDP_ACC.1[1]				●					
FDP_ACC.1[2]						●	●	●	●
FDP_ACC.1[3]			●						
FDP_ACF.1[1]				●					
FDP_ACF.1[2]						●	●	●	●
FDP_ACF.1[3]			●						
FIA_AFL.1[1]				●					
FIA_AFL.1[2]						●	●	●	
FIA_AFL.1[3]	●	●							●
FIA_AFL.1[4]					●				
FIA_SOS.1[1]		●					●		
FIA_SOS.1[2]	●								
FIA_SOS.1[3]					●				
FIA_UAU.2[1]				●					
FIA_UAU.2[2]						●	●	●	
FIA_UAU.2[3]	●	●							●
FIA_UAU.2[4]					●				
FIA_UAU.6	●				●				
FIA_UAU.7	●	●		●	●	●	●	●	●
FIA_UID.2[1]				●					
FIA_UID.2[2]						●	●	●	
FIA_UID.2[3]	●	●							●
FIA_UID.2[4]					●				

TOE Security Function TOE Security Functional Requirement	F.ADMIN-PANEL	F.ADMIN-PC	F.COPY	F.SECURE-PRINT	F.SERVICE	F.BOX-PANEL	F.BOX-PC	F.BOX-UTILITY-1	F.BOX-UTILITY-2
FMT_MOF.1	●								
FMT_MSA.1[1]		●					●		
FMT_MSA.1[2]	●	●							
FMT_MSA.3[1]				●					
FMT_MSA.3[2]							●		
FMT_MSA.3[3]			●						
FMT_MTD.1[1]	●	●							
FMT_MTD.1[2]	●								
FMT_MTD.1[3]		●					●		
FMT_MTD.1[4]					●				
FMT_MTD.1[5]					●				
FMT_SMF.1	●	●			●		●		
FMT_SMR.1[1]							●		
FMT_SMR.1[2]							●		
FMT_SMR.1[3]	●	●							
FMT_SMR.1[4]					●				
FPT_RVM.1	●	●		●	●	●	●	●	●
FPT_SEP.1	●	●	●	●	●	●	●	●	●
FTA_SSL.3[1]	●								
FTA_SSL.3[2]		●							

8.3.1.2. Sufficiency

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

- **FDP_ACC.1[1]**

  FDP_ACC.1[1] regulates the relationship between the controlled subject to the object: secure print job information data file and the operation.

F.SECURE-PRINT executes the operation: “secure print access control” that controls the “print” and “register” to the object: “secure print job information data file” of the subject: “process operating the secure print job.”

Accordingly, this functional requirement is satisfied.

- **FDP_ACC.1[2]**

FDP_ACC.1[2] regulates the relationship between the controlled subject to the object: box and the operation.

F.BOX-PANEL executes the operation: “box access control” controlling the “reading box data within a box” to the object: “box” of the subject: “process operating a box”. (The read box data is transmitted by e-mail or transmitted by FTP.)

F.BOX-PC executes the operation: “box access control” controlling the “reading box data within a box” and “creation” to the object: “box data file” of the subject: “process acting for a general user who is a valid user of the box”. (Read box data is downloaded to the client PC.)

F.BOX-UTILITY-1 executes the operation: “box access control” controlling the “reading box data within a box” to the object: “box” of the subject: “process operating a box”. (Read box data is downloaded to the client PC and is displayed in various formats such as thumbnail display and preview display by a box utility.)

F.BOX-UTILITY-2 executes the operation: “box access control” controlling the “reading box data within a box” and “writing box data to a box” to the object: “box” of the subject: “process operating a box”. (Box data within all boxes is read and downloaded to the client PC. In addition, box data can be written to any box by the client PC.)

Accordingly, this functional requirement is satisfied.

- **FDP_ACC.1[3]**

FDP_ACC.1[3] regulates the relationship between the controlled subject to the object: copy job information data file and the operation.

F.COPY executes the operation: “copy job access control” controlling the “delete” to the object: “copy job information data file” of the subject: “process operating copy job”.

Accordingly, this functional requirement is satisfied.

- **FDP_ACF.1[1]**

  FDP_ACF.1[1] regulates the regulation of the controlled subject: "process operating a secure print job," the object: "secure print job information data file" and the operation: "print" and "register."

  F.SECURE-PRINT creates a newly assigned "job ID" when a secure print job registration request is received, and registers the secure print job information data with this attribute.

  This function also executes control permitting print operation for secure print job information data files having a matching "job ID" to the process operating a secure print job having a "job ID" of the secure print job selected by an authorized general user.

  Accordingly, this functional requirement is satisfied.

- **FDP_ACF.1[2]**

  FDP_ACF.1[2] regulates the regulation of the controlled subject: "process operating a box," the object: "box" and the operation: "reading of box data within a box" and "creation."

  F.BOX-PANEL executes the box access control that the process operating a box having a "box identifier" selected by a general user is permitted the box data reading operation within a box for a box having an identical "box identifier" to the above..

  F.BOX-PC executes the box access control by the following 3 regulations.

  - The process that operates the box having a selected "box identifier" by a general user is permitted the operation of reading the box data in the box to the box having an identical "box identifier" as above.

  - The process that operates the box having the entered "box identifier" is permitted the operation of creating a box having the entered "box identifier" as an object attributes when there is no box having a "box identifier" that is identical to the above.

  - The process that operates the box having the entered "box identifier" executes the denied control of the operation of creating a box having an entered "box identifier" as an object attributes, when there is a box having a "box identifier" that is identical to the above.

F.BOX-UTILITY-1 executes the box access control that the process operating a box having a “box identifier” selected by a general user is permitted the operation reading box data within a box for a box having an identical “box identifier” to the above..

F.BOX-UTILITY-2 executes the box access control by the following 2 regulations.

- The process that operates the box having “administrator identifier” is permitted the operation of reading the box data within a box for all boxes.
- The process that operates the box having “administrator identifier” is permitted the operation of writing the box data within a box for all boxes.

Accordingly, this functional requirement is satisfied.

- **FDP_ACF.1[3]**

FDP_ACF.1[3] regulates the regulation of the controlled subject: “process operating a copy job,” the object: “copy job information data file,” and the operation: “delete.”

F.COPY executes access control deleting after completion of printing the copy job information data files having memory recall settings data set to “Off” by the process operating copy jobs.

- **FIA_AFL.1[1]**

FIA_AFL.1[1] regulates the detection of unauthorized access when a certain number of unsuccessful authentication attempts for the authentication event related to the secure print job information data occurs, and the methods of normal recovery after detection of unauthorized access and the execution of actions.

F.SECURE-PRINT locks the authentication function when 3 unsuccessful authentication attempts are detected for authentication to access secure print job information data. This is released by executing the Access Lock Release Function offered by F.ADMIN-PANEL.
Accordingly, this functional requirement is satisfied.

- **FIA_AFL.1[2]**

FIA_AFL.1[2] regulates the detection of unauthorized access when a certain number of unsuccessful authentication attempts for the authentication event related to the box data occurs, and the methods of normal recovery after detection of unauthorized access and the execution of actions

F.BOX-PANEL locks each authentication functions when 3 unsuccessful authentication attempts are detected for authentication to access to a box. Lock condition is released by execution of the Access Lock Release Function offered by F.ADMIN-PANEL.

F.BOX-PC locks each authentication functions when 3 unsuccessful authentication attempts are detected for authentication to access to a box. Lock condition is released by execution of the Access Lock Release Function offered by F.ADMIN-PANEL.

F.BOX-UTILITY-1 locks each authentication functions when 3 unsuccessful authentication attempts are detected for authentication to access to a box. Lock condition is released by execution of the Access Lock Release Function offered by F.ADMIN-PANEL.
Accordingly, this functional requirement is satisfied.

- **FIA_AFL1[3]**

FIA_AFL1[3] regulates the detection of unauthorized access when a certain number of unsuccessful authentication attempts for the authentication event related to the administrator mode occurs, and the execution of actions after detecting the unauthorized access.

F.ADMIN-PANEL locks the authentication functions when 3 unsuccessful authentication attempts are detected for authentication for accessing administrator mode or for re-authentication for changing an administrator mode password. (This locks the authentication function for accessing the administrator mode after denying access to the administrator mode when re-authenticating for changing an administrator mode password.) In addition, there is no function for releasing this lock.

F.ADMIN-PC locks the authentication functions when 3 unsuccessful authentication attempts are detected for authentication to the administrator mode. In addition, there is no function for releasing this lock.

F.BOX-UTILITY-2 locks the authentication functions when 3 unsuccessful authentication attempts are detected for authentication for requesting the box data backup operation or restore operation. In addition, there is no function for releasing this lock.
Accordingly, this functional requirement is satisfied.

- **FIA_AFL1[4]**

FIA_AFL1[4] regulates the detection of unauthorized access when a certain number of unsuccessful authentication attempts for the authentication event related to the service engineer occurs, and the execution of actions after detecting the unauthorized access.

F.SERVICE locks the authentication functions when 3 unsuccessful authentication attempts are detected for authentication for accessing service mode or for re-authentication for changing a service code. (This locks the authentication function for accessing the service mode after denying access to the service mode when re-authenticating to change a service code.) In addition, there is no function for releasing this lock.
Accordingly, this functional requirement is satisfied.

- **FIA_SOS.1[1]**

  FIA_SOS.1[1] regulates the quality metric of the box password, which is a minimum of 4 digits and a maximum of 64 digits of one-byte English characters or one-byte symbols.
  F.BOX-PC checks whether 4- to 64-digit ASCII code 0x20 to 0x7E (one-byte English characters or one-byte symbols, 95 types) is set as the quality metric of the box password for the function to change the box password.
  F.ADMIN-PC checks whether 4- to 64-digit ASCII code 0x20 to 0x7E (one-byte English characters or one-byte symbols, 95 types) is set as the quality metric of the box password for the function to change the box password.
  Accordingly, this functional requirement is satisfied.

- **FIA_SOS.1[2]**

  FIA_SOS.1[2] regulates the quality metric of the administrator mode password, which is an 8-digit number.
  F.ADMIN-PANEL checks whether an 8-digit number is set as the quality metric for the administrator mode password.
  Accordingly, this functional requirement is satisfied.

- **FIA_SOS.1[3]**

  FIA_SOS.1[3] regulates the quality metric of the service code, which is 8 digits of numbers, “*” or “#.”
  F.SERVICE checks whether 8 digits of numbers, “*” or “#” is set as the quality metric for the service code for the function to change the service code.
  Accordingly, this functional requirement is satisfied.

- **FIA_UAU.2[1]**

  FIA_UAU.2[1] regulates the authentication of a general user who is a valid user of the secure print job, during the access of a general user to the secure print job information data.
  F. SECURE-PRINT authenticates a general user who is a valid user of a secure print job through a secure print password during the access to the secure print job information data, and permits execution of the operations that are available for the

secure print job information data, for which the subject is only an authenticated general user who is the valid user of the secure print job.
Accordingly, this functional requirement is satisfied.

- **FIA_UAU.2[2]**

  FIA_UAU.2[2] regulates the authentication of a general user who is a valid user of the box during the accessing by a general user to the box.
  F. BOX-PANEL authenticates a general user who is a valid user of the box through a box password, and permits the execution of access to the box, for which the subject is only the authenticated general user who is the valid user of the box.
  F. BOX-PC authenticates a general user who is a valid user of the box through a box password, and permits the execution of access to the box, for which the subject is only the authenticated general user who is the valid user of the box.
  F. BOX-UTILITY-1 authenticates a general user who is a valid user of the box through a box password, and permits the execution of access to the box, for which the subject is only the authenticated general user who is the valid user of the box.
  Accordingly, this functional requirement is satisfied.

- **FIA_UAU.2[3]**

  FIA_UAU.2[3] regulates the authentication of an administrator before using administrator functions.
  F. ADMIN-PC authenticates administrators accessing the administrator mode, and permits the execution of operations effective in the administrator mode only to authenticated administrators.
  F. ADMIN-PANEL authenticates administrators accessing the administrator mode, and permits the execution of operations effective in the administrator mode only to authenticated administrators. In addition, administrators are authenticated (re-authenticated) before execution of administrator mode password change functions, which is a security management functions in the administrator mode.
  F. BOX-UTILITY-2 authenticates administrators performing a box data backup operation or restore operation, and permits backup operation or restore operation only to authenticated administrators.
  Accordingly, this functional requirement is satisfied.

- **FIA_UAU.2[4]**

  FIA_UAU.2[4] regulates the authentication of a service engineer before using the service engineer functions.

  F.SERVICE authenticates service engineers during accessing of service mode, and permits the execution of security function operations effective in the service mode only to authenticated service engineers. In addition, it authenticates (re-authenticates)

service engineers before the execution of the service code change function, which is a security management functions in the service mode.
Accordingly, this functional requirement is satisfied.

- **FIA_UAU.6**

FIA_UAU.6 regulates an authentication event that requires re-authentication.
F.ADMIN-PANEL re-authenticates the administrator during the function to change the administrator mode password, which is an important function in terms of the security for the administrator who has already been permitted access to administrator mode, and it permits only a re-authenticated administrator to execute the function to change the administrator mode password.
F.SERVICE re-authenticates the service engineer during the function to change the service code, which is an important function in terms of security for the service engineer who has already been permitted access to service mode, and it permits only a re-authenticated service engineer to execute the function to change the service code.
Accordingly, this functional requirement is satisfied.

- **FIA_UAU.7**

FIA_UAU.7 regulates the return of "*" as feedback during authentication.
F.SECURE-PRINT returns "*" for each character as feedback of the character entry (secure print password) for authentication during access to secure print job information data.
F.BOX-PANEL returns "*" for each character as feedback of the character entry (box password) for authentication during access to the box.
F.BOX-PC returns "*" for each character as feedback of the character entry (box password) for authentication during access to the box.
F.BOX-UTILITY-1 returns "*" for each character as feedback of the character entry (box password) for authentication during access to the box.
F.BOX-UTILITY-2 returns "*" for each character as feedback of the character entry (administrator mode password) for authentication during access of box data backup operation or restore operation request.

F.ADMIN-PANEL returns "*" for each character as feedback of the character entry for the following cases.

- Characters entered for the authentication function during accessing from the MFP body operations panel in administrator mode.
- Characters entered for the re-authentication function when changing an administrator mode password.

F.ADMIN-PC returns “*” for each character as feedback of the character entry (administrator mode password) for authentication during access to the administrator mode from a client PC.

F.SERVICE returns “*” for each character as feedback of the character entry for the following cases.

- Characters entered for the authentication function using the service code for access to the service mode.
- Characters entered for the re-authentication function when changing a service code.

Accordingly, this functional requirement is satisfied.

- **FIA_UID.2[1]**

  FIA_UID.2[1] regulates the identification of the valid user of a secure print job during the accessing of the secure print job information data by a general user.
  F.SECURE-PRINT identifies a general user who is a valid user of the secure print job through the selection of a secure print job, which is the object to be operated by the general user, based on the name of the secure print job, during the accessing of the secure print job information data.
  Accordingly, this functional requirement is satisfied.

- **FIA_UID.2[2]**

  FIA_UID.2[2] regulates the identification of a valid user of a box during the access to the box by a general user handling a box.
  F.BOX-PANEL identifies a general user who is a valid user of the box through the selection of the box name that is set during access of box data.
  F.BOX-PC identifies a general user who is a valid user of the box through the selection of the box name that is set during access of box data.
  F.BOX-UTILITY-1 identifies a general user who is a valid user of the box through the selection of the box name that is set during access of box data.
  Accordingly, this functional requirement is satisfied.

- **FIA_UID.2[3]**

  FIA_UID.2[3] regulates the identification of an administrator before use of administrator functions.
  F.ADMIN-PANEL identifies the user as an administrator by the access request of the user to the administrator mode.
  F.ADMIN-PC identifies the user as an administrator by the access request of the user to the administrator mode.

F.BOX-UTILITY-2 identifies the user as an administrator by the request of the box data backup operation or restore operation.
Accordingly, this functional requirement is satisfied.

- **FIA_UID.2[4]**

  FIA_UID.2[4] regulates the identification of a user as a service engineer before use of service engineer functions.
  F.SERVICE identifies the user as a service engineer by access request of the user to the service mode (execution of an operation procedure that is not public).
  Accordingly, this functional requirement is satisfied.

- **FMT_MOF.1**

  FMT_MOF.1 regulates the behavior management of the Unauthorized Access Lock Function by the administrator.
  F.ADMIN-PANEL provides a settings management function that enables and disables the Unauthorized Access Lock Function.
  Accordingly, this functional requirement is satisfied.

- **FMT_MSA.1[1]**

  FMT_MSA.1[1] regulates the limitation on the operation to change the box identifier that is a security attribute used in box access control, to “general users who are valid user of the box” and administrators.
  F.ADMIN-PC provides a function to change the box identifier by administrator mode.
  F.BOX-PC provides a function to change the box identifier operated by a general user who is the valid user permitted to access the box.
  Accordingly, this functional requirement is satisfied.

- **FMT_MSA.1[2]**

  FMT_MSA.1[2] regulates the limitation on the default modification and query of memory recall settings data that is a security attribute used in copy job access control, to administrators.

  F.ADMIN-PANEL provides a function to query or change (change default values) memory recall settings data.
  F.ADMIN-PC provides a function to query or change (change default values) memory recall settings data by administrator mode.
  Accordingly, this functional requirement is satisfied.

- **FMT_MSA.3[1]**

  FMT_MSA.3[1] regulates the default values during the creation of job ID which is security attributes used by secure print access control, and the roles overwriting default values.

F.SECURE-PRINT distinguishes secure prints spooled to the MFP as separate from other jobs and assigns to the secure print job a value that can be uniquely identified. There is no role changing a job ID because there is no necessity to change a job ID once it has been created.
Accordingly, this functional requirement is satisfied.

- **FMT_MSA.3[2]**

  FMT_MSA.3[2] regulates the permitted default value during the creation of a box identifier, which is a security attribution used during box access control. In addition, it regulates the limitation on the role of setting an initial value that replaces the default value to the general user who creates the user box.
  F.BOX-PC provides a blank (null) as a default value for the box identifier when the box creation function is started, and it also provides a box identifier creation function to set an alternative default value to the blank for the general user who creates the box.
  Accordingly, this functional requirement is satisfied.

- **FMT_MSA.3[3]**

  FMT_MSA.3[3] regulates the default values during the creation of memory recall setting data which is security attributes used by copy job access control, and the roles overwriting default values.
  F.COPY assigns memory recall settings data set by “ Off ” (no memory recall) corresponding to control characteristics for copy job information data files created during execution of copies.
  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[1]**

  FMT_MTD.1[1] regulates the role changing the administrator mode passwords and auto reset settings data.

  F.ADMIN-PANEL provides a function to change an administrator mode password in the administrator mode accessing from the MFP body operations panel. Also, it provides a function to change auto reset operational setting data.
  F.ADMIN-PC provides a function to change auto reset settings data in the administrator mode accessing from a client PC.
  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[2]**

  FMT_MTD.1[2] regulates the role deleting unauthorized access detection count values for secure prints and unauthorized access detection count values for boxes.
  F.ADMIN-PANEL provides Access Lock Release Function operated by an administrator in administrator mode. This function clears to zero the unauthorized

access detection count value of each secure print job and the unauthorized access detection count value of each box.
Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[3]**

  FMT_MTD.1[3] regulates the role changing a box password.
  F.ADMIN-PC provides a function to change the box password operated by an administrator in administrator mode.
  F.BOX-PC provides a function to change a box password operated by a general user who is a valid user of the box.
  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[4]**

  FMT_MTD.1[4] regulates the role changing a service code.
  F.SERVICE provides a function to change the service code operated by a service engineer in service mode.
  Accordingly, this functional requirement is satisfied.

- **FMT_MTD.1[5]**

  FMT_MTD.1[5] regulates the role initializing an administrator mode password.
  F.SERVICE provides a function to initialize an administrator mode password operated by the service engineer in service mode. When this function is executed, a default value during set up is set as the administrator mode password.
  Accordingly, this functional requirement is satisfied.

- **FMT_SMF.1**

  FMT_SMF.1 regulates the security management functions that are provided by the TOE.
  F.BOX-PC provides the following security management functions, operated by a general user who is the valid user of the box, for the box.

  - Function to change the box identifier of the box
  - Function to change the box password for the box

  In addition, F.BOX-PC provides the following security management functions for a general user who creates the box, during the creation of a box.

  - Function to create a box identifier

  F.ADMIN-PANEL provides the following security management functions operated by the administrator in administrator mode.

  - Operation setting function for the Unauthorized Access Lock Function
  - Access Lock Release Function that clears the detected unauthorized access count value for a secure print to zero

- Access Lock Release Function that clears the detected unauthorized access count value for a box to zero
- Function to change the administrator mode password
- Settings management function for Auto Reset Operational Settings Data
- Settings management function for memory recall settings data

F.ADMIN-PC provides the following security management functions operated by the administrator in administrator mode.

- Function to change the box identifier of any box
- Function to change the box password of any box
- Settings management function for Auto Reset Operational Settings Data
- Settings management function for memory recall settings data

F.SERVICE provides the following security management functions operated by the service engineer in service mode.

- Function to change the service code
- Initialization function for the administrator mode password.

Accordingly, this functional requirement is satisfied.

- **FMT_SMR.1[1]**

  FMT_SMR.1[1] regulates the role as a “ general user creating the corresponding box. ”
  F.BOX-PC recognizes the user who has activated the box creation function during creation of a box as the “ general user who creating the corresponding box ” .
  Accordingly, this functional requirement is satisfied.

- **FMT_SMR.1[2]**

  FMT_SMR.1[2] regulates the role as a “general user who is the valid user of the box.”
  F.BOX-PC recognizes the identified and authenticated user as the “ general user who is the valid user of the corresponding box ” for access to the corresponding box.
  Accordingly, this functional requirement is satisfied.

- **FMT_SMR.1[3]**

  FMT_SMR.1[3] regulates the role as an “administrator”
  F.ADMIN-PANEL recognizes an authenticated user as the “administrator” for access to administrator mode.
  F.ADMIN-PC recognizes an authenticated user as the “administrator” for access to administrator mode.

Accordingly, this functional requirement is satisfied.

- **FMT_SMR.1[4]**

  FMT_SMR.1[4] regulates the role as a "service engineer"
  F.SERVICE recognizes an authenticated user as the "service engineer" for access to service mode.
  Accordingly, this functional requirement is satisfied.

- **FPT_RVM.1**

  FPT_RVM.1 regulates support so that the TSP enforcement functions are always invoked before each security function within the TOE is allowed to proceed.

  F.ADMIN-PANEL and F.ADMIN-PC always execute a function that authenticates the user accessing the administrator mode as an administrator before enabling operation of security management functions in the administrator mode. In addition, the function to change the administrator mode password provided by F.ADMIN-PANEL executes a function to re-authenticate the administrator before its execution is permitted. The box data backup function and restore function provided by F.BOX-UTILITY-2 executes functions to authenticate the user before operation is permitted. These authentication functions are TSP enforcement functions that operate before each security function is allowed to proceed, resulting in a mechanism that is always in operation.

  F.SECURE-PRINT always executes functions that identify and authenticate a general user who is the valid user of the secure print job information data file, which is the print target, before secure print job information data file is permitted to print. These identification and authentication functions are TSP enforcement functions that operate before print operation by secure print job access control function is permitted, resulting in a mechanism that is always in operation.

  F.SERVICE always executes a function that authenticates that the user who is accessing the service mode is a service engineer before enabling operation of security management functions in the service mode. In addition, the function to change the service code provided by F.SERVICE executes a function to re-authenticate the service engineer before the execution is permitted. These authentication functions are TSP enforcement functions operated before each security function is permitted to proceed, resulting in a mechanism that is always in operation.

  F.BOX-PANEL, F.BOX-PC, and F.BOX-UTILITY-1 always execute functions that identify and authenticate a general user who is the valid user of the box that is the operation target before permitting box access. The identification and authentication functions for access to the box are TSP enforcement functions that are executed before permitting operation of box access control functions and reading of box data within a box, resulting in a mechanism that is always in operation.

Therefore, each TSP enforcement function is always invoked before permitting advancement of functions controlled by all of the identified TOE security functions. Accordingly, this functional requirement is satisfied.

- **FPT_SEP.1**

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

With F.ADMIN-PANEL, the administrator mode that is the security domain maintained after administrator identification and authentication, cannot be interfered by subjects not trusted.

With F.ADMIN-PC, the administrator mode that is the security domain maintained after administrator identification and authentication, cannot be interfered by subjects not trusted.

With F.COPY, the security domain that is maintained during execution of copy job access control, cannot be interfered by subjects not trusted.

With F.SECURE-PRINT, the security domain that is maintained during execution of secure print job access control executed after authentication of a general user who is a valid user of a secure print job, cannot be interfered by subjects not trusted.

With F.SERVICE, the service mode that is the security domain maintained after service engineer identification and authentication, does not receive any access from another subject.

With F.BOX-PANEL, the security domain after box access authentication cannot be interfered by subjects not trusted.

With F.BOX-PC, the security domain after box access authentication cannot be interfered by subjects not trusted. In addition, access by multiple users to a single box is permitted, but the security domains that are maintained by each permitted valid user are separated and it cannot be interfered.

With F.BOX-UTILITY-1, the security domain after box access authentication cannot be interfered by subjects not trusted. In addition, access by multiple users to a single box is permitted, but the security domains that are maintained by each permitted valid user are separated and it cannot be interfered.

With F.BOX-UTILITY-2, the security domain that is maintained after administrator identification and authentication cannot be interfered by subjects not trusted.

Therefore, each of the security domains is not interfered with and thus, this functional requirement is satisfied.

- **FTA_SSL.3[1]**

  FTA_SSL.3[1] regulates administrator mode connected session termination that is accessing from the MFP body operations panel.

  F.ADMIN-PANEL automatically blocks access to the administrator mode when inactive for the established period (None, 0~9 minutes) set by auto reset operation settings data during connecting to administrator mode from the MFP body operations panel.

  Accordingly, this functional requirement is satisfied.

- **FTA_SSL.3[2]**

  FTA_SSL.3[2] regulates administrator mode connected session termination that is accessing from a client PC.

  F.ADMIN-PC automatically blocks access to the administrator mode when inactive for the established period (1~4 minutes set: 5 minutes, 5~9 minutes set: setting value, no setting: 10 minutes) set by auto reset operation settings data during connecting to administrator mode from a client PC.

  Accordingly, this functional requirement is satisfied.

8.3.2. Rationale for TOE Security Strength of Function

The TOE security functions having a probabilistic/permutational mechanism are (1) the administrator mode password authentication mechanism by F. ADMIN-PANEL, F.ADMIN-PC and F.BOX-UTILITY-2, (2) the secure print password authentication mechanism by F.SECURE-PRINT, (3) the service code authentication mechanism provided by F.SERVICE and (4) the box password authentication mechanism by F.BOX-PANEL, F.BOX-PC, and F.BOX-UTILITY-1. Each authentication mechanism has a password space of (1) an 8-digit number, (2) a 4-digit number, (3) 8 digits of number or "#" or "*," and (4) 4 to 64 digit ASCII code 0x20 to 0x7E (95 types of characters), respectively, and operates along with the Unauthorized Access Lock Function. (Three unsuccessful authentication attempts lock the access. See Section 6.1 for details. Note, when the service code authentication mechanism detects three unsuccessful trials it locks the access regardless of the operation setting of the Unauthorized Access Lock Function.) Accordingly, as claimed in Section 6.2, the strength of function of the mechanisms adequately satisfies the SOF-Basic, and it is consistent with the minimum strength of function: SOF-Basic that is claimed for the TOE security functional requirement for the security strength of function, stipulated in item 5.1.2.

8.3.3. Mutually Supported TOE Security Functions

The TOE security functional requirements that are satisfied by a combination of IT security functions that are identified in the TOE summary specifications, are as shown in the text regarding the rationale in the section of 8.3.1.2.

8.3.4. Rationale for Assurance Measures

The required document for the evaluation assurance level EAL3 is covered by the reference document shown in the assurance measures described in Section 6.3. The TOE security assurance requirements are satisfied through development, test conduction, vulnerability analysis, the development environment control, configuration management, life cycle management, and delivery procedures in accordance with the document provided as the assurance measures, as well as the preparation of a proper guidance document.

8.4. PP claims rationale

There is no PP that is referenced by this ST.

~ LAST PAGE ~