

EPSON  
LX-10020M/WF-M21000 with FAX  
Security Target

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

ST Version: Rev.05  
Created on: July 30, 2021  
Created by: SEIKO EPSON CORPORATION

## Revision History

| Rev. | Revised Section   | Revision Details   | Design Dept. |               |             | Creation/Revision Date |
|------|---|--|--------------|---------------|-------------|------------------------|
|      |   |  | Created by   | Checked by    | Approved by |                        |
| 01   | · Entire document   | · Newly create   | Yoshioka     | Kawahara Niki | Narusawa    | 2021/03/12             |
| 02   | · Chapters 1.1, 1.4<br>· Chapters 6.1, 7.4<br>· Chapters 6.1, 7.2           | · Alteration of matters pointed out for revision<br>· Alteration of matters pointed out for revision<br>· Error correction                               | Yoshioka     | Kawahara Niki | Narusawa    | 2021/04/05             |
| 03   | · Chapters 1.1, 1.2, 1.4  | · Error correction   | Yoshioka     | Kawahara Niki | Narusawa    | 2021/05/12             |
| 04   | · Chapters 1.1, 1.4   | · Error correction   | Yoshioka     | Kawahara Niki | Narusawa    | 2021/05/28             |
| 05   | · Chapters 1.1, 1.4, 1.5<br>· Chapters 3.1, 3.3, 3.4<br>· Chapters 3.5, 6.3 | · Alteration of matters pointed out for revision<br>· Alteration of matters pointed out for revision<br>· Alteration of matters pointed out for revision | Yoshioka     | Kawahara Niki | Narusawa    | 2021/07/30             |
|      |   |  |              |               |             |                        |
|      |   |  |              |               |             |                        |
|      |   |  |              |               |             |                        |
|      |   |  |              |               |             |                        |
|      |   |  |              |               |             |                        |

## Contents

|        |   |    |
|--------|---|----|
| 1.     | ST Introduction.....  | 4  |
| 1.1.   | ST Reference.....   | 4  |
| 1.2.   | TOE Reference.....  | 4  |
| 1.3.   | TOE Overview.....   | 4  |
| 1.3.1. | TOE Type.....   | 4  |
| 1.3.2. | TOE Usage.....  | 4  |
| 1.3.3. | Major Security Functions of TOE.....  | 6  |
| 1.4.   | TOE Description.....  | 7  |
| 1.4.1. | Definition of Users.....  | 7  |
| 1.4.2. | Physical Boundary of TOE.....   | 7  |
| 1.4.3. | Logical Boundary of TOE.....  | 10 |
| 1.4.4. | Hardware/software/firmware other than the TOE but that is required for the TOE..... | 12 |
| 1.5.   | Terminology/Abbreviations.....  | 13 |
| 2.     | Conformance Claims.....   | 15 |
| 2.1.   | CC Conformance Claim.....   | 15 |
| 2.2.   | PP Conformance Claim.....   | 15 |
| 2.3.   | Package Conformance Claim.....  | 15 |
| 2.4.   | SFR Package functions.....  | 15 |
| 2.5.   | SFR Package attributes.....   | 16 |
| 2.6.   | PP Conformance Rationale.....   | 16 |
| 2.6.1. | Consistency Claim with TOE Type in PP.....  | 16 |
| 2.6.2. | Consistency Claim with Security Problems and Security Objectives in PP.....         | 17 |
| 2.6.3. | Consistency Claim with Security Requirements in PP.....                             | 17 |
| 3.     | Security Problem Definition.....  | 19 |
| 3.1.   | Protected Assets.....   | 19 |
| 3.2.   | Threats agents.....   | 20 |
| 3.3.   | Threats to TOE Assets.....  | 21 |
| 3.4.   | Organizational Security Policies for the TOE.....                                   | 21 |
| 3.5.   | Assumptions.....  | 21 |
| 4.     | Security Objectives.....  | 23 |
| 4.1.   | Security Objectives for the TOE.....  | 23 |
| 4.2.   | Security Objectives for the IT environment.....                                     | 23 |
| 4.3.   | Security Objectives for the non-IT environment.....                                 | 24 |
| 4.4.   | Security Objectives rationale.....  | 24 |
| 5.     | Extended components definition.....   | 29 |
| 5.1.   | FPT_FDI_EXP Restricted forwarding of data to external interfaces.....               | 29 |
| 6.     | Security Requirements.....  | 31 |

|        |   |    |
|--------|---|----|
| 6.1.   | Security Functional Requirements .....                | 31 |
| 6.1.1. | Class FAU: Security audit.....                        | 31 |
| 6.1.2. | Class FDP: User data protection .....                 | 33 |
| 6.1.3. | Class FIA: Identification and authentication .....    | 37 |
| 6.1.4. | Class FMT: Security management .....                  | 41 |
| 6.1.5. | Class FPT: Protection of the TSF .....                | 47 |
| 6.1.6. | Class FTA: TOE access .....                           | 48 |
| 6.1.7. | Class FTP: Trusted paths/channels .....               | 48 |
| 6.2.   | Security Assurance Requirements .....                 | 49 |
| 6.3.   | Security Requirements Rationale.....                  | 49 |
| 6.3.1. | Security Functional Requirements rationale.....       | 50 |
| 6.3.2. | Security Assurance Requirements rationale.....        | 55 |
| 6.3.3. | Dependency Analysis .....                             | 55 |
| 7.     | TOE Summary Specification .....                       | 57 |
| 7.1.   | User Identification and Authentication Function ..... | 57 |
| 7.2.   | Document Access Control Function .....                | 59 |
| 7.3.   | Access Control Function for TOE Function .....        | 65 |
| 7.4.   | Security Management Function .....                    | 67 |
| 7.5.   | Residual Data Overwrite Function .....                | 69 |
| 7.6.   | Self-Test Function .....                              | 69 |
| 7.7.   | Audit Log Function .....                              | 70 |
| 7.8.   | Network Protection Function .....                     | 71 |

## 1. ST Introduction

This section describes the ST reference, TOE reference, TOE overview, and TOE description.

### 1.1. ST Reference

ST title: EPSON LX-10020M/WF-M21000 with FAX Security Target  
ST version: Rev.05  
Created: 2021/07/30  
Created by: SEIKO EPSON CORPORATION

### 1.2. TOE Reference

The TOE identification information is shown below.

TOE name: EPSON LX-10020M/WF-M21000 with FAX  
TOE version: 1.00  
Manufacturer: SEIKO EPSON CORPORATION

The TOE is composed of the MFP (Japan: LX-10020M; overseas: WF-M21000), the fax (Japan: Super G3/G3 Multi Fax Board/PR3FB0; overseas: Super G3/G3 Multi Fax Board/PR3FB1), and the firmware (GR12L4). The TOE can be verified by the model number of the MFP, the identification information of the fax, and the identification information of the firmware.

### 1.3. TOE Overview

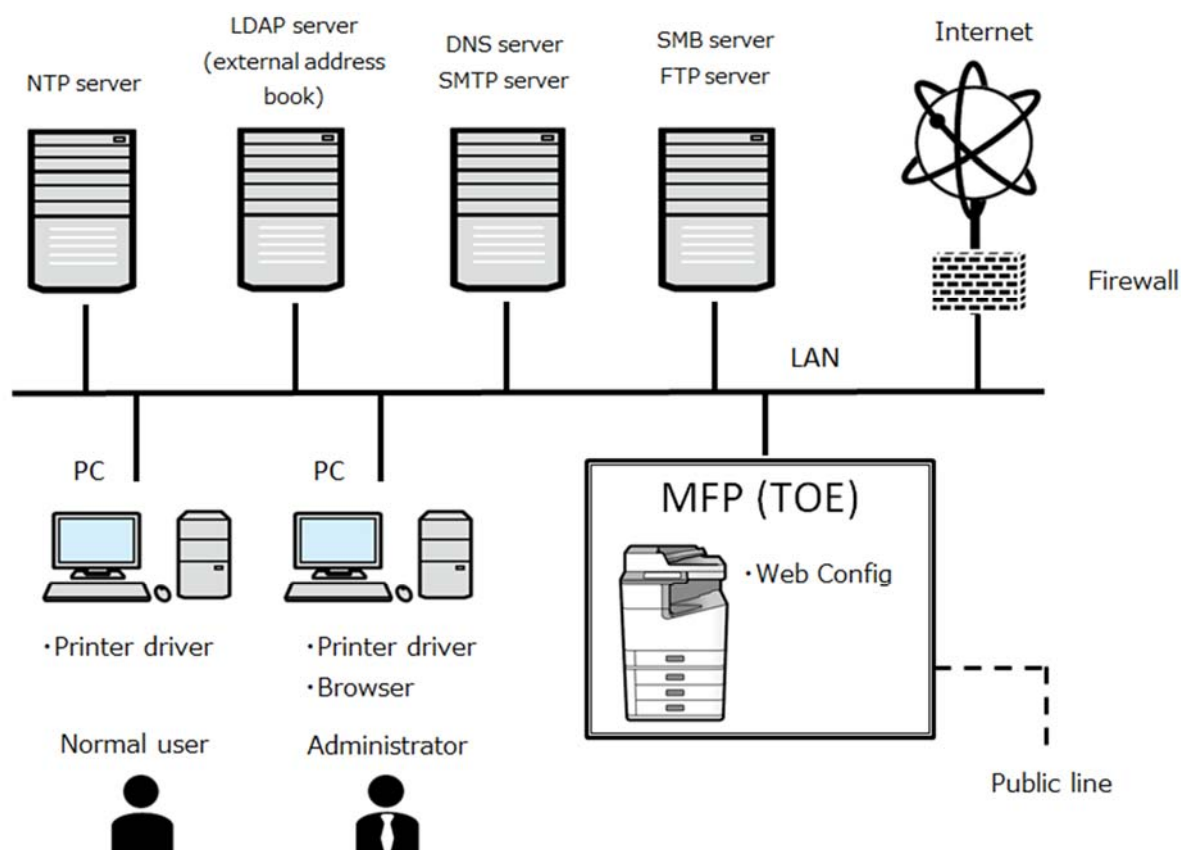
This section defines TOE type, TOE usage and major security functions of the TOE.

#### 1.3.1. TOE Type

The TOE defined in this ST is a digital Multi Function Peripheral (MFP) that is used in a LAN environment and has print, scan, copy, fax, and document storage functions.

#### 1.3.2. TOE Usage

Figure 1-1 shows the usage environment for this TOE.



**Figure 1-1 TOE Usage Environment**

The TOE is connected to a LAN and a public line. The user can operate the TOE with the operation panel that the TOE is equipped with or via the LAN. The elements of Figure 1-1 are explained below.

(1) MFP

An MFP (Multi Function Peripheral) is a peripheral device for computers that has multiple different functions (printer, scanner, copying, fax, etc.).

(2) LAN

A LAN (Local Area Network) is a network that connects computers, communication devices, printers, and other such equipment in the same building using cables, wireless, and other methods to transfer data.

(3) Public line

A public line is a general telephone subscriber line, and is used to send and receive faxes.

(4) Firewall

A firewall is a piece of software, device, system, or other such item that is installed at the point where a computer or network comes into contact with an external network and relays and monitors incoming and outgoing communication to protect the internal network from attacks from external locations.

(5) PC

A PC (Personal Computer) is a compact, low-cost general-purpose computer product for individuals.

(6) NTP server

An NTP (Network Time Protocol) server is a piece of server software that delivers data with the current time.

(7) LDAP server (external address book)

An LDAP server is a piece of server software that uses the LDAP (Light Directory Access Protocol) to access the directory services used as standard on TCP/IP networks such as the Internet. It also refers to an actual physical server on which such LDAP server software is running. The LDAP server manages an address book which is used to specify recipients of fax data.

(8) DNS server/SMTP server

A DNS server is a piece of server software that uses a DNS (Domain Name System) to convert the name of servers on an internal network into an IP address. It also refers to an actual physical server on which such DNS server software is running. An SMTP server is a piece of server software that uses the SMTP (Simple Mail Transfer Protocol) to send email that is used as standard on TCP/IP networks such as the Internet. It also refers to an actual physical server on which such SMTP server software is running. It is used to send mail containing scan data. DNS servers and SMTP servers can be installed independently of each other.

(9) SMB server/FTP server

An SMB server is a piece of server software that uses a SMB (Server Message Block) to perform actions such as sharing files or printers between multiple Windows computers on a network (LAN). It also refers to an actual physical server on which such SMB server software is running.

An FTP server is a piece of server software that uses the FTP (File Transfer Protocol) to send and receive files. It also refers to an actual physical server on which such FTP server software is running. Both servers are used for the transfer of scan data and fax receiving data.

These servers are used for the transfer of scan data and receiving of fax data.

(10) Printer driver

A printer driver is a piece of software that is required to connect and operate a printer from a computer. It is a type of device driver that adds hardware control functions to operating system, and a separate one is normally required for each type of printer and each type of operating system.

(11) Browser

A browser is a piece of software for viewing compiled data and information.

(12) Web Config

This is a function embedded in MFPs manufactured by Seiko Epson. This function makes it possible to configure a range of settings (print settings, network settings, user restriction settings, administrator password, etc.) for a printer or MFP by accessing it by its IP address from a browser.

### 1.3.3. Major Security Functions of TOE

The major security functions of the TOE are as below.

(1) User Identification and Authentication Function

A function to identify and authenticate users of the TOE

(2) Document Access Control Function

A function to restrict operations on user data

(3) Access Control Function for TOE Function

A function to control TOE functions

(4) Security Management Function

A function to manage security functions

(5) Residual Data Overwrite Function

A function to completely erase deleted or temporarily stored documents from an HDD or Flash ROM and make them unrecoverable

(6) Self-Test Function

A function that verifies part of TSF and TSF implementation code are normal when the MFP starts up

(7) Audit Log Function

A function that records TOE usage and security-related events as an audit log for reference

(8) Network Protection Function

A function to prevent information leakage and data tampering from the network due to eavesdropping when using the LAN

#### 1.4. TOE Description

This section describes user definitions, the physical boundary of the TOE, guidance, the logical boundary of the TOE, and the hardware/software/firmware other than TOE but that is required for the TOE.

##### 1.4.1. Definition of Users

Table 1-1 describes the users for this TOE

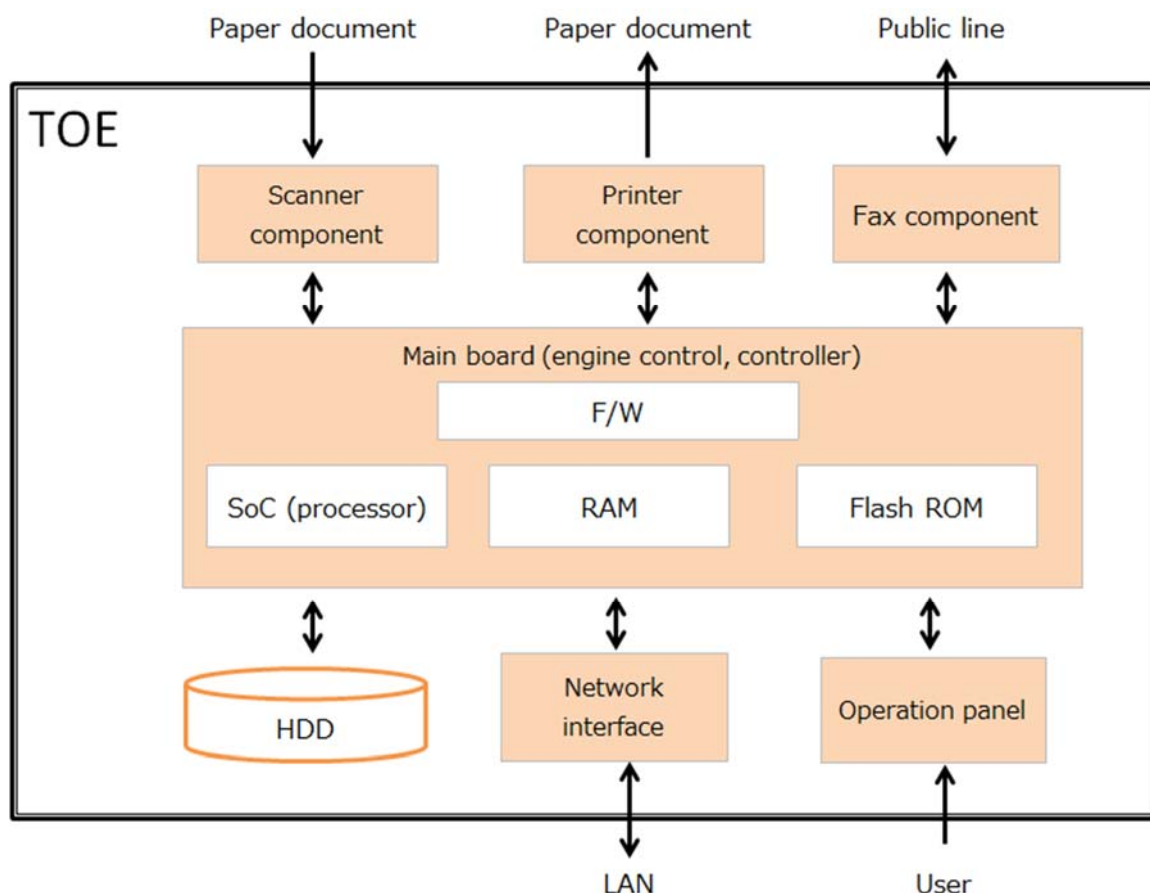
**Table 1-1 User Definitions**

| Name           |                                  | Definition   |
|----------------|----------------------------------|--|
| U.USER<br>User |                                  | Any authorized User.   |
|                | U.NORMAL<br>Normal user          | A User who is authorized to perform User Document Data processing functions of the TOE.  |
|                | U.ADMINISTRATOR<br>Administrator | A User who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TOE security policy (TSP). Administrators may possess special privileges that provide capabilities to override portions of the TSP. |

##### 1.4.2. Physical Boundary of TOE

Figure 1-2 shows the physical boundary of this TOE.





**Figure 1-2 Physical Boundary of this TOE**

The TOE is an MFP that is composed of a main board, a printer component, a scanner component, a fax component, a network interface, and operation panel and an HDD. The elements of Figure 1-2 are explained below.

(1) Main Board

The main board is a component on which are installed at a very high density things such as electronic components, integrated circuits (IC), and metal wiring to connect these.

(2) F/W

F/W (Firmware) is a type of software embedded in a computer or other device and has functions that perform basic control of things such as internal circuits and devices.

(3) SoC (processor)

An SoC (processor) is a device that performs control of various devices and calculation and processing of data. It executes a program that is stored in memory, receives data from input devices and storage devices, and after performing computations and processing, outputs it to an output device or storage device.

(4) RAM

RAM (Random Access Memory) is a memory device from which data can be erased and rewritten. It can read or write data anywhere in the device in the same time (i.e. random access), but data in this memory

disappears when the power is turned off.

(5) Flash ROM

Flash ROM (Read Only Memory) is a memory device from which data can be erased and rewritten. Data in this memory does not disappear when the power is turned off.

(6) Printer Component

The printer component is a component that controls print functions.

(7) Scanner Component

The scanner component is a component that controls scan functions.

(8) Fax Component

The fax component is a component that controls fax functions. The fax boards described in Table 1-2 provide these functions.

(9) Network Interface

The network interface is a device that is required to connect the MFP to a LAN.

(10) Operation Panel

The operation panel is a user interface device to operate the MFP.

(11) HDD

An HDD (Hard Disk Drive) is a device that stores data.

Table 1-2 shows the delivery methods for the components of the TOE.

**Table 1-2 Delivery methods for components of the TOE**

| Component of TOE | Format                    | Delivery method                    | Identification information  |
|------------------|---------------------------|------------------------------------|---|
| MFP              | MFP device                | Delivered by courier               | <ul style="list-style-type: none"> <li>• Japan: LX-10020M</li> <li>• Overseas: WF-M21000</li> </ul>   |
| Fax              | Fax board                 | Delivered by courier               | <ul style="list-style-type: none"> <li>• Japan: Super G3/G3 Multi Fax Board/ PR3FB0</li> <li>• Overseas: Super G3/G3 Multi Fax Board/ PR3FB1</li> </ul> |
| Guidance         | Format shown in Table 1-3 | Delivery method shown in Table 1-3 | Name and version shown in Table 1-3   |
| Firmware         | Digital file              | Delivered by service personnel     | Version GR12L4  |

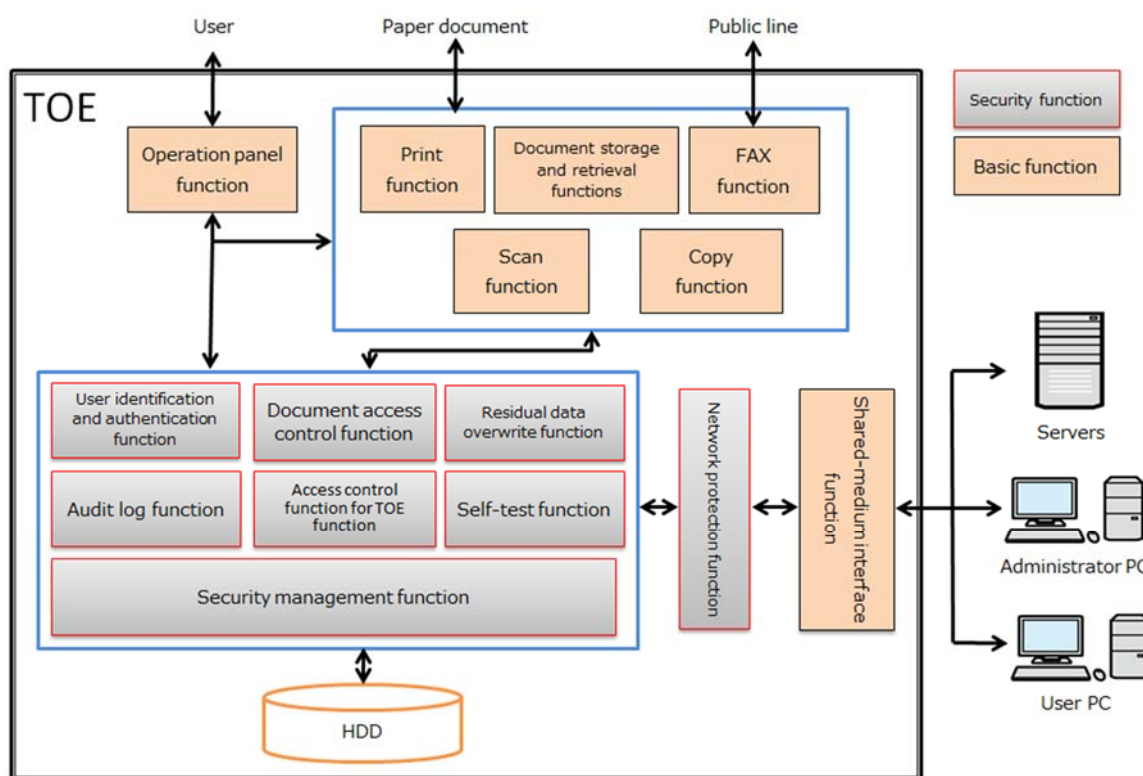
Table 1-3 shows the guidance that comprises this TOE.

**Table 1-3 List of Guidance Comprising the TOE**

| Name                        | Ver.          | Format           | Delivery method   | Target market  |
|-----------------------------|---------------|------------------|-------------------|----------------|
| User's Guide                | NPD6659-02 JA | PDF format files | Delivery over web | Japan          |
| Supplemental Security Guide | NPD6692-01 JA | PDF format files | Delivery over web | Japan          |
| Before Use                  | 4140894-00    | Paper media      | Packaged with MFP | Japan/overseas |
| User's Guide                | NPD6658-02 EN | PDF format files | Delivery over web | Overseas       |
| Supplemental Security Guide | NPD6692-01 EN | PDF format files | Delivery over web | Overseas       |

### 1.4.3.Logical Boundary of TOE

Figure 1-3 shows the logical boundary of this TOE.

**Figure 1-3 Logical Boundary of the TOE**

The elements in Figure 1-3 are explained below.

◆ Basic functions provided by the TOE

(1) Print Function

A function to print digital documents received from a client via a LAN

## (2) Scan Function

A function to read a paper document and generate a digital document from it based on operations by a user on the operation panel

## (3) Copy Function

A function to read a paper document and print a copy image of it based on operations by a user on the operation panel

## (4) Fax Function

A function to send digital documents to an external fax (fax sending function), and a function to receive digital documents from an external fax (fax receiving function)

- Fax Sending Function

A function to send a digital document over a public line to an external fax device

- Fax Receiving Function

A function to receive a digital document over a public line from an external fax device

## (5) Document Storage and Retrieval Functions

A function, called a box function, to save digital documents within the TOE and retrieve the saved digital documents

- A function to save digital documents in personal boxes

A function to save digital documents read from the scanner or digital documents specified on a PC to be saved to a personal box

- A function to retrieve and use digital documents that have been saved to a personal box

A function used by which digital documents saved to a personal box can be retrieved, printed, previewed, deleted, or sent to other systems

## (6) Shared-medium Interface Functions

A function for TOE users to remotely control the TOE from a client PC

## (7) Operation Panel Function

A function to control the operation panel

◆ Security functions provided by the TOE

## (1) User Identification and Authentication Function

A function to identify and authenticate users who input their user name and logon password on an operation panel or via a network. This function includes functions for administrators to set the minimum number and required character types for logon passwords and functions to protect authentication feedback by displaying dummy characters when logon passwords are input. Furthermore, it includes functions to lock out targeted accounts a specified time period after authentication fails, and functions to automatically log off if no operations occur for a specified time period after logon.

## (2) Document Access Control Function

A control function that allows users to operate user data and job data in the TOE according to the rights assigned to each user or to the rights assigned to the role of a user that has been authenticated by the

User Identification and Authentication Function.

(3) Access Control Function for TOE Function

A control function that allows only permitted users to use the basic functions of the TOE based on the access control rules for users that have been authenticated by the User Identification and Authentication Function. The basic functions of the TOE are as follows.

- Print function
- Scan function
- Copy function
- Fax receiving and sending functions
- Document storage and retrieval functions

(4) Security Management Function

The Security Management Function is a function to manage the following items based on the rights assigned to roles through the operation panel or network.

- Security Attributes
- TSF data
- Management Functionality
- User roles

(5) Residual Data Overwrite Function

A function to make residual information impossible to reuse by overwriting it with a specified value after the data has been deleted by users or after the data has been saved to an HDD or flash ROM, and is no longer needed, while using the basic functions, such as print, scan, copy, and fax, of the TOE.

(6) Self-Test Function

A function to detect illegal modifications to the TOE firmware and to verify that parts of the TSF data and TSF implementation codes are complete and that parts of the TSF operate normally when the TOE starts up.

(7) Audit Log Function

A function that records a log of security-related events and a history of who, when, and how the TOE is operated. The log, which is a readable file format that only administrators can audit, can be downloaded and deleted, but the audit log itself is stored on the TOE and cannot be edited, even by administrators.

(8) Network Protection Function

A function that uses IPsec encrypted communications to prevent information leakage and data tampering due to eavesdropping on the network while the TOE is communicating with various servers and client PCs via wired LAN. Functions are also provided so the TOE does not directly transfer information between telephone lines and wired LAN without additional processing by TSF.

#### 1.4.4. Hardware/software/firmware other than the TOE but that is required for the TOE

To use the TOE, the following software and the hardware on which they run are required.

**Table 1-4 Non-TOE Software Required for the TOE**

| Software       | Version used for evaluation  |
|----------------|--|
| NTP server     | Microsoft Windows Server 2016 Standard   |
| LDAP server    | Microsoft Windows Server 2016 Standard   |
| DNS server     | Microsoft Windows Server 2016 Standard   |
| SMTP server    | hMailServer 5.6.7-B2425  |
| SMB server     | Microsoft Windows Server 2016 Standard   |
| FTP server     | Microsoft Windows Server 2016 Standard   |
| Printer driver | For Microsoft Windows<br>Japanese version: Epson Printing System (J) Version 3.01.00<br>English version: Epson Printing System (A) Version 3.01.00 |
| Browser        | Microsoft Edge   |

\*The letter in the brackets for the English version of the printer driver indicates the time zone of the PC on which it is installed.

If the time zone of the PC used is not North America, a "W" is displayed in the brackets, but this is the same driver.

### 1.5. Terminology/Abbreviations

Table 1-5 defines the meaning of the specific terminology and abbreviations in this ST.

**Table 1-5 Terminology/Abbreviations**

| Glossary                 | Definition  |
|--------------------------|---|
| User ID of normal users  | Attributes assigned to U.NORMAL, D.DOC, and D.FUNC<br>A unique identifier is assigned to U.NORMAL   |
| User role                | Attribute assigned to U.USER<br>There are normal users and administrator<br>Normal users are assigned to U.NORMAL, and administrator is assigned to U.ADMINISTRATOR   |
| Available Function List  | Attribute assigned to U.NORMAL<br>For U.NORMAL, a list of functions for which usage is permitted is assigned<br>The functions are print (PRT), scan (SCAN), copy (CPY), fax receiving (FAXIN), fax sending (FAXOUT), and document storage and retrieval (DSR) |
| MFP function             | A collective name for print, scan, copy, fax, and document storage and retrieval functions provided by the TOE  |
| Function type            | Attributes assigned to MFP functions<br>Print attributes, scan attributes, copy attributes, fax attributes, and document storage and retrieval attributes   |
| Document data attributes | Attributes assigned to D.DOC, and D.FUNC<br>There are print, scan, copy, fax receiving, fax sending, and document storage and   |

|                    |   |
|--------------------|---|
|                    | retrieval   |
| Job                | A processing unit from the start to the end of processing by the MFP function on a D.DOC    |
| Password Print Job | A print job to which User IDs of normal users and passwords of normal users have been added |

## 2. Conformance Claims

This section describes Conformance Claim.

### 2.1. CC Conformance Claim

The CC conformance claim for this ST is detailed below.

Common Criteria version: Version 3.1 Release 5

Common Criteria conformance: Part 2 extended and Part 3 conformant

### 2.2. PP Conformance Claim

The PP conformance claim for this ST is detailed below.

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

PP version: 1.0

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

### 2.3. Package Conformance Claim

The package conformance claim for this ST is detailed below.

This ST conforms to Common Criteria Evaluation Assurance Level (EAL) 2 augmented by ALC\_FLR.2.SFR  
Packages conform to PP are as follows.

- 2600.2-PRT, SFR Package for Hardcopy Device Print Functions, Operational Environment B (Package Version 1.0, dated March 2009)
- 2600.2-SCN, SFR Package for Hardcopy Device Scan Functions, Operational Environment B (Package Version 1.0, dated March 2009)
- 2600.2-CPY, SFR Package for Hardcopy Device Copy Functions, Operational Environment B (Package Version 1.0, dated March 2009)
- 2600.2-FAX, SFR Package for Hardcopy Device FAX Functions, Operational Environment B (Package Version 1.0, dated March 2009)
- 2600.2-DSR, SFR Package for Hardcopy Device Document Storage and Retrieval (DSR) Functions, Operational Environment B (Package Version 1.0, dated March 2009)
- 2600.2-SMI, SFR Package for Hardcopy Device Shared-medium Interface Functions, Operational Environment B (Package Version 1.0, dated March 2009)

### 2.4. SFR Package functions

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



**Table 2-1 SFR Package Functions**

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

## 2.5. SFR Package attributes

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

**Table 2-2 SFR Package Attributes**

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

## 2.6. PP Conformance Rationale

This section sets forth the consistency claim with TOE type in PP, the consistency claim with PP security problems and security objectives, and the consistency claim with PP security requirements.

### 2.6.1.Consistency Claim with TOE Type in PP

This TOE is an MFP that has print, scan, copy, fax, document storage and retrieval, and shared-medium interface functions, so its type is consistent with the hardcopy device (HCD) noted in "2600.2, Protection Profile

for Hardcopy Devices, Operational Environment B." The TOE does not have a removable HDD or any other non-volatile storage system, so of the seven SFR packages defined in "2600.2, Protection Profile for Hardcopy Devices, Operational Environment B", it conforms to all but "2600.2-NVS, SFR Package for Hardcopy Device Nonvolatile Storage Functions, Operational Environment B."

### 2.6.2.Consistency Claim with Security Problems and Security Objectives in PP

The security problems in this ST are exactly the same as in the security problems demanded to be solved in the PP, and are consistent. In terms of security objectives, OE.AUDIT\_STORAGE.PROTECTED and OE.AUDIT\_ACCESS.AUTHORIZED are deleted from the security objectives of the IT environment, and O.AUDIT\_STORAGE.PROTECTED and O.AUDIT\_ACCESS.AUTHORIZED are added as the security objectives for the TOE. The internal functions that implement O.AUDIT\_STORAGE.PROTECTED and O.AUDIT\_ACCESS.AUTHORIZED are equivalent to the demands in OE.AUDIT\_STORAGE.PROTECTED and OE.AUDIT\_ACCESS.AUTHORIZED.

### 2.6.3.Consistency Claim with Security Requirements in PP

Table 2-3 shows the SFR demanded in the PP and the SFR stipulated in this ST.

**Table 2-3 SFR Relationship**

| SFR demanded in PP | SFR stipulated in this ST |
|--------------------|---------------------------|
| FAU_GEN.1          | FAU_GEN.1                 |
| FAU_GEN.2          | FAU_GEN.2                 |
|                    | FAU_SAR.1                 |
|                    | FAU_SAR.2                 |
|                    | FAU_STG.1                 |
|                    | FAU_STG.4                 |
| FDP_ACC.1(a)       | FDP_ACC.1(a)              |
| FDP_ACC.1(b)       | FDP_ACC.1(b)              |
| FDP_ACF.1(a)       | FDP_ACF.1(a)              |
| FDP_ACF.1(b)       | FDP_ACF.1(b)              |
| FDP_RIP.1          | FDP_RIP.1                 |
|                    | FIA_AFL.1                 |
| FIA_ATD.1          | FIA_ATD.1                 |
|                    | FIA_SOS.1                 |
| FIA_UAU.1          | FIA_UAU.1                 |
|                    | FIA_UAU.7                 |
| FIA_UID.1          | FIA_UID.1                 |
| FIA_USB.1          | FIA_USB.1                 |
| FMT_MSA.1(a)       | FMT_MSA.1(a)              |
| FMT_MSA.1(b)       | FMT_MSA.1(b)              |

|               |               |
|---------------|---------------|
| FMT_MSA.3(a)  | FMT_MSA.3(a)  |
| FMT_MSA.3(b)  | FMT_MSA.3(b)  |
| FMT_MTD.1     | FMT_MTD.1     |
| FMT_SMF.1     | FMT_SMF.1     |
| FMT_SMR.1     | FMT_SMR.1     |
| FPT_FDI_EXP.1 | FPT_FDI_EXP.1 |
| FPT_STM.1     | FPT_STM.1     |
| FPT_TST.1     | FPT_TST.1     |
| FTA_SSL.3     | FTA_SSL.3     |
| FTP_ITC.1     | FTP_ITC.1     |

Having conformed with all SFR demanded in the PP, this ST adds several additional SFR. And with the exception of FDP\_ACF.1.3(b), all SFR in the PP are completely the same as the SFR stipulated in the ST. In FDP\_ACF.1.3(b) in the PP, administrator permissions can be used to permit the user performing operations to operate all TOE functions, whereas this ST places restrictions on some print functions. As such, FDP\_ACF.1.3(b) in this ST is more restrictive than FDP\_ACF.1.3(b) in the PP.

The PP also defines the modify and delete operations on D.FUNC in the Common Access Control SFP. However, in this TOE, the modify operation is not permitted for D.FUNC. This is a more restricted access control than the PP.

As such, as this ST is equivalent to or more restrictive than the PP, it is demonstrably compliant with the PP.

### 3. Security Problem Definition

This section describes Protected assets, Threats, Organizational Security Policies and Assumptions.

#### 3.1. Protected Assets

Protected assets refer to user data, TSF data, and functions.

##### (1) User Data

User data refers to data that is created by the user and does not have any impact on TOE security functions. It is divided into the following two categories.

**Table 3-1 User Data**

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

##### (2) TSF Data

TSF data refers to data that has an impact on TOE security functions. It is divided into the following two categories.

**Table 3-2 TSF Data**

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

Table 3-3 shows the TSF data in the scope of this TOE.

**Table 3-3 TSF Data in the Scope of this TOE**

| Name   | TSF data in this ST                              | Details  |
|--------|--|--|
| D.PROT | User ID of normal users                          | U.NORMAL identification information  |
|        | Administrator user ID                            | U.ADMINISTRATOR identification information<br>The identifier "Administrator" is assigned |
|        | List of recipients for scan/fax/email or address | Address book   |

|        |   |  |
|--------|---|--|
|        | book  |  |
|        | Job status log  | Job history  |
|        | Password policy   | Settings information concerning password character types and number of digits                  |
|        | Non-operation timer setting   | Time information for automatic ending of logon session from operation panel                    |
|        | Administrator authentication settings (operation panel)                   | Settings information to activate/disable administrator authentication from the operation panel |
|        | User restriction settings   | Information for settings that can be configured from Web Config (inc. Available Function List) |
|        | IPsec settings  | Settings information concerning IPsec  |
|        | Time settings   | Time settings information  |
|        | Network settings  | Network settings information   |
|        | Hash value for verifying integrity of firmware                            | Hash value calculated from the firmware file<br>Stored in TOE                                  |
| D.CONF | Normal user passwords   | U.NORMAL authentication information  |
|        | Administrator password  | U.ADMINISTRATOR authentication information   |
|        | Passwords to access external devices such as a mail server or file server | Password to access a mail server<br>Password to access a file server                           |
|        | Audit log   | Log information generated by the monitoring log function                                       |
|        | IPsec preshared key   | Cryptographic key required for key exchange in IPsec   |

### (3) Functions

Functions refers to the function in Table 2-1.

#### 3.2. Threats agents

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

- Persons who are not permitted to use the TOE who may attempt to use the TOE.
- Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.
- Persons who are authorized to use the TOE who may attempt to access data in ways for which they are not authorized.
- Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

The threats and policies defined in this Security Target address the threats posed by these threat agents.

### 3.3. Threats to TOE Assets

This section describes threats to assets described in 3.1.

**Table 3-4 Threats to User Data for the TOE**

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

**Table 3-5 Threats to TSF Data for the TOE**

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

### 3.4. Organizational Security Policies for the TOE

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

**Table 3-6 Organizational Security Policies for the TOE**

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

### 3.5. Assumptions

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

**Table 3-7 Assumptions for the TOE**

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

#### 4. Security Objectives

This section describes Security Objectives for TOE, Security Objectives of Operational Environment and Security Objectives Rationale.

##### 4.1. Security Objectives for the TOE

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

**Table 4-1 Security Objectives for the TOE**

| Objective                 | Definition  |
|---------------------------|---|
| O.DOC.NO_DIS              | The TOE shall protect User Document Data from unauthorized disclosure.  |
| O.DOC.NO_ALT              | The TOE shall protect User Document Data from unauthorized alteration.  |
| O.FUNC.NO_ALT             | The TOE shall protect User Function Data from unauthorized alteration.  |
| O.PROT.NO_ALT             | The TOE shall protect TSF Protected Data from unauthorized alteration.  |
| O.CONF.NO_DIS             | The TOE shall protect TSF Confidential Data from unauthorized disclosure.   |
| O.CONF.NO_ALT             | The TOE shall protect TSF Confidential Data from unauthorized alteration.   |
| O.USER.AUTHORIZED         | The TOE shall require identification and authentication of Users and shall ensure that Users are authorized in accordance with security policies before allowing them to use the TOE. |
| O.INTERFACE.MANAGED       | The TOE shall manage the operation of external interfaces in accordance with security policies.   |
| O.SOFTWARE.VERIFIED       | The TOE shall provide procedures to self-verify executable code in the TSF.   |
| O.AUDIT.LOGGED            | The TOE shall create and maintain a log of TOE use and security-relevant events and prevent its unauthorized disclosure or alteration.  |
| O.AUDIT_STORAGE.PROTECTED | The TOE shall ensure that audit records are protected from unauthorized access, deletion and modifications.   |
| O.AUDIT_ACCESS.AUTHORIZED | The TOE shall ensure that audit records can be accessed in order to detect potential security violations, and only by authorized persons.   |

##### 4.2. Security Objectives for the IT environment

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



**Table 4-2 Security Objectives for the IT Environment**

| Objective            | Definition  |
|----------------------|---|
| OE.INTERFACE.MANAGED | The IT environment shall provide protection from unmanaged access to TOE external interfaces. |

#### 4.3. Security Objectives for the non-IT environment

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

**Table 4-3 Security Objectives for the Non-IT Environment**

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

#### 4.4. Security Objectives rationale

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

Table 4-4 Completeness of Security Objectives

|                         | O.DOC.NO_DIS | O.DOC.NO_ALT | O.FUNC.NO_ALT | O.PROT.NO_ALT | O.CONF.NO_DIS | O.CONF.NO_ALT | O.USER.AUTHORIZED | O.INTERFACE.MANAGED | O.SOFTWARE.VERIFIED | O.AUDIT.LOGGED | O.AUDIT_STORAGE.PROTECTED | O.AUDIT_ACCESS.AUTHORIZED | OE.INTERFACE.MANAGED | OE.PHYSICAL.MANAGED | OE.USER.AUTHORIZED | OE.USER.TRAINED | OE.ADMIN.TRAINED | OE.ADMIN.TRUSTED | OE.AUDIT.REVIEWED |
|-------------------------|--------------|--------------|---------------|---------------|---------------|---------------|-------------------|---------------------|---------------------|----------------|---------------------------|---------------------------|----------------------|---------------------|--------------------|-----------------|------------------|------------------|-------------------|
| T.DOC.DIS               | ✓            |              |               |               |               |               | ✓                 |                     |                     |                |                           |                           |                      |                     | ✓                  |                 |                  |                  |                   |
| T.DOC.ALT               |              | ✓            |               |               |               |               | ✓                 |                     |                     |                |                           |                           |                      |                     | ✓                  |                 |                  |                  |                   |
| T.FUNC.ALT              |              |              | ✓             |               |               |               | ✓                 |                     |                     |                |                           |                           |                      |                     | ✓                  |                 |                  |                  |                   |
| T.PROT.ALT              |              |              |               | ✓             |               |               | ✓                 |                     |                     |                |                           |                           |                      |                     | ✓                  |                 |                  |                  |                   |
| T.CONF.DIS              |              |              |               |               | ✓             |               | ✓                 |                     |                     |                |                           |                           |                      |                     | ✓                  |                 |                  |                  |                   |
| T.CONF.ALT              |              |              |               |               |               | ✓             | ✓                 |                     |                     |                |                           |                           |                      |                     | ✓                  |                 |                  |                  |                   |
| P.USER.AUTHORIZATION    |              |              |               |               |               |               | ✓                 |                     |                     |                |                           |                           |                      |                     | ✓                  |                 |                  |                  |                   |
| P.SOFTWARE.VERIFICATION |              |              |               |               |               |               |                   |                     | ✓                   |                |                           |                           |                      |                     |                    |                 |                  |                  |                   |
| P.AUDIT.LOGGING         |              |              |               |               |               |               |                   |                     |                     | ✓              | ✓                         | ✓                         |                      |                     |                    |                 |                  |                  | ✓                 |
| P.INTERFACE.MANAGEMENT  |              |              |               |               |               |               |                   | ✓                   |                     |                |                           |                           | ✓                    |                     |                    |                 |                  |                  |                   |
| A.ACCESS.MANAGED        |              |              |               |               |               |               |                   |                     |                     |                |                           |                           |                      | ✓                   |                    |                 |                  |                  |                   |
| A.USER.TRAINING         |              |              |               |               |               |               |                   |                     |                     |                |                           |                           |                      |                     |                    | ✓               |                  |                  |                   |
| A.ADMIN.TRAINING        |              |              |               |               |               |               |                   |                     |                     |                |                           |                           |                      |                     |                    |                 | ✓                |                  |                   |
| A.ADMIN.TRUST           |              |              |               |               |               |               |                   |                     |                     |                |                           |                           |                      |                     |                    |                 |                  | ✓                |                   |

Table 4-5 Sufficiency of Security Objectives

| Threats, policies, and assumptions | Summary  | Objectives and rationale   |
|------------------------------------|--|--|
| T.DOC.DIS                          | User Document Data may be disclosed to unauthorized persons. | O.DOC.NO_DIS protects D.DOC from unauthorized disclosure.  |
|                                    |  | O.USER.AUTHORIZED establishes user identification and authentication as the basis for authorization. |
|                                    |  | OE.USER.AUTHORIZED establishes responsibility of the TOE Owner to appropriately grant authorization. |

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

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

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

## 5. Extended components definition

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

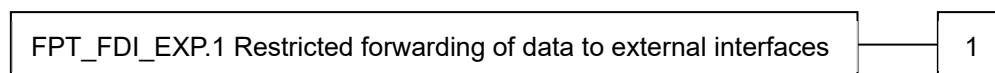
### 5.1. FPT\_FDI\_EXP Restricted forwarding of data to external interfaces

#### Family behavior:

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

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

#### Component leveling:



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

#### Management: FPT\_FDI\_EXP.1

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

- a) Definition of the role(s) that are allowed to perform the management activities
- b) Management of the conditions under which direct forwarding can be allowed by an administrative role
- c) Revocation of such an allowance

#### Audit: FPT\_FDI\_EXP.1

The following actions should be auditable if FAU\_GEN Security Audit Data Generation is included in the PP/ST: There are no auditable events foreseen.

#### Rationale:

Quite often, a TOE is supposed to perform specific checks and process data received on one external interface before such (processed) data are allowed to be transferred to another external interface. Examples are firewall

systems but also other systems that require a specific work flow for the incoming data before it can be transferred. Direct forwarding of such data (i.e., without processing the data first) between different external interfaces is therefore a function that—if allowed at all—can only be allowed by an authorized role.

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

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

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

#### **FPT\_FDI\_EXP.1 Restricted forwarding of data to external interfaces**

**Hierarchical to:** No other components

**Dependencies:** FMT\_SMF.1 Specification of Management Functions  
FMT\_SMR.1 Security roles

**FPT\_FDI\_EXP.1.1** The TSF shall provide the capability to restrict data received on [assignment: *list of external interfaces*] from being forwarded without further processing by the TSF to [assignment: *list of external interfaces*].

## 6. Security Requirements

This section describes Security Functional Requirements, Security Assurance Requirements and Security Requirements Rationale.

### 6.1. Security Functional Requirements

This section describes the operation results for security function requirements.

#### 6.1.1. Class FAU: Security audit

##### **FAU\_GEN.1 Audit data generation**

**Hierarchical to:** No other components

**Dependencies:** FPT\_STM.1 Reliable time stamps

**FAU\_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and
- **all Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 6-1;** [assignment: *other specifically defined auditable events*]

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

- not specified

[assignment: *other specifically defined auditable events*]

- None

**Table 6-1 Auditable Events**

| Auditable Event   | Relevant SFR | Audit level | Additional information                   | Details  |
|---|--------------|-------------|--|--|
| Use of authentication mechanism fail<br>Use of authentication mechanism success | FIA_UAU.1    | Basic       | None                                     | Logon operation fail<br>Logon operation success  |
| Use of identification mechanism fail<br>Use of identification mechanism success | FIA_UID.1    | Basic       | User identification test (if applicable) | Logon operation fail (inc. user identification information)<br>Logon operation success |
| Use of management functions   | FMT_SMF.1    | Minimum     | None                                     | Management function (see Table 6-11) record  |
| Modification of user group that plays a partial role                            | FMT_SMR.1    | Minimum     | None                                     | No modification so no records  |



|   |           |         |                                    |                          |
|---|-----------|---------|------------------------------------|--------------------------|
| Change of time                                | FPT_STM.1 | Minimum | None                               | Change of time           |
| Failure of communication with trusted channel | FTP_ITC.1 | Minimum | Communication recipient IP address | IPsec communication fail |

**FAU\_GEN.1.2** The TSF shall record within each audit record at least the following information:

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

[assignment: *other audit relevant information*]

- None

**FAU\_GEN.2** **User identity association**

**Hierarchical to:** No other components

**Dependencies:** FAU\_GEN.1 Audit data generation

FIA\_UID.1 Timing of identification

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

**FAU\_SAR.1** **Audit review**

**Hierarchical to:** No other components

**Dependencies:** FAU\_GEN.1 Audit data generation

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

[assignment: *authorised users*]

- Administrator

[assignment: *list of audit information*]

- Table 6-1 shows auditable events

**FAU\_SAR.1.2** The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

**FAU\_SAR.2** **Restricted audit review**

**Hierarchical to:** No other components

|                    |   |
|--------------------|---|
|                    | <b>Dependencies:</b> FAU_SAR.1 Audit review   |
| <b>FAU_SAR.2.1</b> | The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.  |
| <b>FAU_STG.1</b>   | <b>Protected audit trail storage</b>  |
|                    | <b>Hierarchical to:</b> No other components   |
|                    | <b>Dependencies:</b> FAU_GEN.1 Audit data generation  |
| <b>FAU_STG.1.1</b> | The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.   |
| <b>FAU_STG.1.2</b> | The TSF shall be able to [selection, choose one of: <i>prevent</i> , <i>detect</i> ] unauthorized modifications to the stored audit records in the audit trail.   |
|                    | [selection, choose one of: <i>prevent</i> , <i>detect</i> ]   |
|                    | – prevent   |
| <b>FAU_STG.4</b>   | <b>Prevention of audit data loss</b>  |
|                    | <b>Hierarchical to:</b> FAU_STG.3 Action in case of possible audit data loss  |
|                    | <b>Dependencies:</b> FAU_STG.1 Protected audit trail storage  |
| <b>FAU_STG.4.1</b> | The TSF shall [selection, choose one of: “ <i>ignore audited events</i> ”, “ <i>prevent audited events, except those taken by the authorised user with special rights</i> ”, “ <i>overwrite the oldest stored audit records</i> ”] and [assignment: <i>other actions to be taken in case of audit storage failure</i> ] if the audit trail is full. |
|                    | [selection, choose one of: “ <i>ignore audited events</i> ”, “ <i>prevent audited events, except those taken by the authorised user with special rights</i> ”, “ <i>overwrite the oldest stored audit records</i> ”]  |
|                    | – overwrite the oldest stored audit records   |
|                    | [assignment: <i>other actions to be taken in case of audit storage failure</i> ]  |
|                    | – None  |

#### 6.1.2.Class FDP: User data protection

|                       |  |
|-----------------------|--|
| <b>FDP_ACC.1(a)</b>   | <b>Subset access control</b>   |
|                       | <b>Hierarchical to:</b> No other components  |
|                       | <b>Dependencies:</b> FDP_ACF.1 Security attribute based access control   |
| <b>FDP_ACC.1.1(a)</b> | The TSF shall enforce the Common Access Control SFP in Table 6-2 on the list of users as subjects, objects, and operations among subjects and objects covered by the Common Access Control SFP in Table 6-2. |
| <b>FDP_ACC.1(b)</b>   | <b>Subset access control</b>   |
|                       | <b>Hierarchical to:</b> No other components  |

**Dependencies:** FDP\_ACF.1 Security attribute based access control

**FDP\_ACC.1.1(b)** The TSF shall enforce the **TOE Function Access Control SFP in Table 6-3 on users as subjects, TOE functions as objects, and the right to use the functions as operations.**

**FDP\_ACF.1(a) Security attribute based access control**

**Hierarchical to:** No other components

**Dependencies:** FDP\_ACC.1 Subset access control

**FMT\_MSA.3 Static attribute initialisation**

**FDP\_ACF.1.1(a)** The TSF shall enforce the **Common Access Control SFP in Table 6-2** to objects based on the following: **the list of users as subjects and objects controlled under the Common Access Control SFP in Table 6-2, and for each, the indicated security attributes in Table 6-2.**

**FDP\_ACF.1.2(a)** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules specified in the Common Access Control SFP in Table 6-2 governing access among controlled users as subjects and controlled objects using controlled operations on controlled objects.**

**Table 6-2 Rules Controlling Operations between Controlled Subjects and Objects**

| Object | Document data attributes                | Operation      | Subject  | Rules Controlling Operation  |
|--------|---|----------------|----------|--|
| D.DOC  | +PRT<br>+SCN<br>+CPY<br>+FAXOUT<br>+DSR | Delete<br>Read | U.NORMAL | Denied, except for his/her own documents<br><br>Documents are owned by the U.NORMAL that created the document  |
|        | +FAXIN                                  | Delete<br>Read | U.NORMAL | Denied, except for his/her own documents<br><br>Received fax documents are owned by the U.NORMAL assigned by the "Fax Receiving Function (FAXIN)" in the Available Function List |
| D.FUNC | +PRT<br>+SCN<br>+CPY<br>+FAXOUT<br>+DSR | Delete         | U.NORMAL | Denied, except for his/her own documents<br><br>Documents are owned by the U.NORMAL that created the document  |
|        |   | Modify         | U.NORMAL | Denied   |
|        | +FAXIN                                  | Delete         | U.NORMAL | Denied, except for his/her own   |

|  |  |        |          |   |
|--|--|--------|----------|---|
|  |  |        |          | documents<br>Received fax documents are owned by the U.NORMAL assigned by the "Fax Receiving Function (FAXIN)" in the Available Function List |
|  |  | Modify | U.NORMAL | Denied  |

**FDP\_ACF.1.3(a)** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:  
[assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].

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

- For a U.ADMINISTRATOR, the "Delete" operation is permitted for D.DOC with the document data attribute "+PRT".
- For a U.ADMINISTRATOR, the "Read" and "Delete" operations are permitted for D.DOC with the document data attributes "+SCN", "+CPY", "+FAXIN", "+FAXOUT", and "+DSR"
- For a U.ADMINISTRATOR, the "Delete" operation is permitted for D.FUNC with the document data attributes "+PRT", "+SCN", "+CPY", "+FAXIN", "+FAXOUT", and "+DSR"

**FDP\_ACF.1.4(a)** The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

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

- For a U.ADMINISTRATOR, the "Modify" operation is not permitted for D.FUNC with the document data attributes "+PRT", "+SCN", "+CPY", "+FAXIN", "+FAXOUT", and "+DSR"

**FDP\_ACF.1(b) Security attribute based access control**

**Hierarchical to:** No other components

**Dependencies:** FDP\_ACC.1 Subset access control

FMT\_MSA.3 Static attribute initialisation

**FDP\_ACF.1.1(b)** The TSF shall enforce the TOE **Function Access Control SFP** to objects based on the following:  
**users and** [assignment: *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP*].

[assignment: *list of TOE functions and the security attribute(s) used to determine the TOE Function Access Control SFP*]

- See Table 6-3

**FDP\_ACF.1.2(b)** The TSF shall enforce the following rules to determine if an operation among controlled subjects and

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

[selection: *the user is explicitly authorized by U.ADMINISTRATOR to use a function, a user that is authorized to use the TOE is automatically authorized to use the functions* [assignment: *list of functions*], [assignment: *other conditions*]]

– [assignment: *other conditions*]

[assignment: *other conditions*]

– See Table 6-3

**Table 6-3 Rules Controlling Operations between Controlled Subjects and Objects**

| Object | Operation                     | Subject  | Security Attribute  | Rules Controlling Operation  |
|--------|-------------------------------|----------|---|--|
| F.PRT  | Job execution<br>Job deletion | U.NORMAL | Available Function List (PRT)                                       | For subjects to which the print function (PRT) is assigned in the Available Function List, operation is permitted  |
| F.SCN  | Job execution<br>Job deletion | U.NORMAL | Available Function List (SCN)                                       | For subjects to which the scan function (SCN) is assigned in the Available Function List, operation is permitted   |
| F.CPY  | Job execution<br>Job deletion | U.NORMAL | Available Function List (CPY)                                       | For subjects to which the copy function (CPY) is assigned in the Available Function List, operation is permitted   |
| F.FAX  | Job execution<br>Job deletion | U.NORMAL | Available Function List (FAXIN)<br>Available Function List (FAXOUT) | For subjects to which the fax receiving function (FAXIN) and fax sending function (FAXOUT) are assigned in the Available Function List, operation is permitted |
| F.DSR  | Job execution<br>Job deletion | U.NORMAL | Available Function List (DSR)                                       | For subjects to which the document storage and retrieval function (DSR) is assigned in the Available Function List, operation is permitted                     |

**FDP\_ACF.1.3(b)** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

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

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

- For a U.ADMINISTRATOR, the "Job deletion" operation is permitted for "F.PRT"
- For a U.ADMINISTRATOR, the "Job execution" and "Job deletion" operations are permitted for "F.SCN", "F.CPY", "F.FAX", and "F.DSR"

**FDP\_ACF.1.4(b)** The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

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

- None

#### **FDP\_RIP.1      Subset residual information protection**

**Hierarchical to:**    **No other components**

**Dependencies:**      **No dependencies**

**FDP\_RIP.1.1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] the following objects: **D.DOC**, [assignment: *list of objects*].

[selection: *allocation of the resource to, deallocation of the resource from*]

- deallocation of the resource from

[assignment: *list of objects*]

- None

#### 6.1.3.Class FIA: Identification and authentication

#### **FIA\_AFL.1      Authentication failure handling**

**Hierarchical to:**    **No other components**

**Dependencies:**      **FIA\_UAU.1 Timing of authentication**

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

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

- [assignment: *positive integer number*]

[assignment: *positive integer number*]

- 1

[assignment: *list of authentication events*]

- Logon from the operation panel by an administrator

- Logon from the operation panel by a normal user
- Logon from Web Config by an administrator
- Authentication upon receipt of a Password Print Job

**FIA\_AFL.1.2** When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].

[selection: *met, surpassed*]

- met

[assignment: *list of actions*]

- See Table 6-4

**Table 6-4 Action List**

| Logon Pattern                                       | Action upon unsuccessful authentication             |
|---|---|
| Logon from the operation panel by an administrator  | Lock the relevant administrator out for 0.6 seconds |
| Logon from the operation panel by a normal user     | Lock the relevant normal user out for 0.6 seconds   |
| Logon from Web Config by an administrator           | Lock the relevant administrator out for 1 second    |
| Authentication upon receipt of a Password Print Job | Lock the relevant normal user out for 1 second      |

**FIA\_ATD.1** **User attribute definition**

**Hierarchical to:** No other components

**Dependencies:** No dependencies

**FIA\_ATD.1.1** The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

[assignment: *list of security attributes*]

- See Table 6-5

**Table 6-5 Security Attribute List**

| User            | Security Attribute  |
|-----------------|---|
| U.NORMAL        | User ID of normal users<br>User role<br>Available Function List |
| U.ADMINISTRATOR | User role   |

**FIA\_SOS.1 Verification of secrets****Hierarchical to:** No other components**Dependencies:** No dependencies

**FIA\_SOS.1.1** The TSF shall provide a mechanism to verify that secrets (normal user passwords, administrator password) meet [assignment: *a defined quality metric*].

[assignment: *a defined quality metric*]

- Length: 8 characters or more (maximum 20)
- Character types: must include at least one of the following character types
  - Upper-case letters
  - Lower-case letters
  - Numbers
  - Symbols (!"#\$%&'()\*+,-./:;<=>?@[¥]^\_`{|}~ )

**FIA\_UAU.1 Timing of authentication****Hierarchical to:** No other components**Dependencies:** FIA\_UID.1 Timing of identification

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

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

- Printer information display on operation panel
- Printer information print from operation panel
- Network information display on operation panel
- Network information print from operation panel
- Job list display on operation panel
- Help display on operation panel
- Printer information display on Web Config
- Network information display on Web Config
- Fax information display on operation panel
- Fax information print from operation panel
- Printer maintenance function execution from operation panel
- Printer status display on printer driver

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



**FIA\_UAU.7 Protected authentication feedback****Hierarchical to:** No other components**Dependencies:** FIA\_UAU.1 Timing of authentication

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

[assignment: *list of feedback*]

- See Table 6-6

**Table 6-6 Feedback List**

| Action   | Feedback   |
|--|--|
| Logon from the operation panel by an administrator | * characters equaling the number of characters entered   |
| Logon from the operation panel by a normal user    | * characters equaling the number of characters entered   |
| Logon from Web Config by an administrator          | Mask characters equaling the number of characters entered<br>*Masked character types depend on the browser |

**FIA\_UID.1 Timing of identification****Hierarchical to:** No other components**Dependencies:** No dependencies

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

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

- Printer information display on operation panel
- Printer information print from operation panel
- Network information display on operation panel
- Network information print from operation panel
- Job list display on operation panel
- Help display on operation panel
- Printer information display on Web Config
- Network information display on Web Config
- Fax information display on operation panel
- Fax information print from operation panel
- Printer maintenance function execution from operation panel

- Printer status display on printer driver

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

**FIA\_USB.1 User-subject binding**

**Hierarchical to:** No other components

**Dependencies:** FIA\_ATD.1 User attribute definition

**FIA\_USB.1.1** The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *list of user security attributes*].

[assignment: *list of user security attributes*]

- See Table 6-5

**FIA\_USB.1.2** The TSF shall enforce the following rules on the initial association of user security attributes with the subjects acting on behalf of users: [assignment: *rules for the initial association of attributes*].

[assignment: *rules for the initial association of attributes*]

- None

**FIA\_USB.1.3** The TSF shall enforce the following rules governing changes to the user security attributes with the subjects acting on behalf of users: [assignment: *rules for the changing of attributes*].

[assignment: *rules for the changing of attributes*]

- None

#### 6.1.4.Class FMT: Security management

**FMT\_MSA.1(a) Management of security attributes**

**Hierarchical to:** No other components

**Dependencies:** [FDP\_ACC.1 Subset access control, or  
FDP\_IFC.1 Subset information flow control]

FMT\_SMR.1 Security roles

FMT\_SMF.1 Specification of Management Functions

**FMT\_MSA.1.1(a)** The TSF shall enforce the **Common Access Control SFP in Table 6-2**, [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change\_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].

- [assignment: *access control SFP(s), information flow control SFP(s)*]
- None
- [selection: *change\_default, query, modify, delete, [assignment: other operations]*]
- See Table 6-7
  - [assignment: other operations]
- [assignment: *other operations*]
- See Table 6-7
- [assignment: *list of security attributes*]
- See Table 6-7
- [assignment: *the authorized identified roles*]
- See Table 6-7

**Table 6-7 Security Attributes, Operations, and User Roles for which Operations are Permitted**

| Security Attribute       | Operation                       | User role for which operation is permitted |
|--------------------------|---------------------------------|--|
| User ID of normal users  | [Selected operations] delete    | U.ADMINISTRATOR                            |
|                          | [Added operations] Newly create |  |
| User role                | [Selected operations] modify    | Nobody                                     |
| Available Function List  | [Selected operations] modify    | U.ADMINISTRATOR                            |
| Document data attributes | [Selected operations] modify    | Nobody                                     |

**FMT\_MSA.1(b) Management of security attributes**

**Hierarchical to:** No other components

**Dependencies:** [FDP\_ACC.1 Subset access control, or  
FDP\_IFC.1 Subset information flow control]

**FMT\_SMR.1 Security roles**

**FMT\_SMF.1 Specification of Management Functions**

**FMT\_MSA.1.1(b)** The TSF shall enforce the **TOE Function Access Control SFP in Table 6-3**, [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change\_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

- [assignment: *access control SFP(s), information flow control SFP(s)*]
- None
- [selection: *change\_default, query, modify, delete, [assignment: other operations]*]
- See Table 6-8
- [assignment: *list of security attributes*]
- See Table 6-8

[assignment: *the authorised identified roles*]

- See Table 6-8

**Table 6-8 Security Attributes, Operations, and User Roles for which Operations are Permitted**

| Security Attribute      | Operation                    | User role for which operation is permitted |
|-------------------------|------------------------------|--|
| User role               | [Selected operations] modify | Nobody                                     |
| Available Function List | [Selected operations] modify | U.ADMINISTRATOR                            |
| Function type           | [Selected operations] modify | Nobody                                     |

**FMT\_MSA.3(a) Static attribute initialisation**

**Hierarchical to:** No other components

**Dependencies:** FMT\_MSA.1 Management of security attributes

FMT\_SMR.1 Security roles

**FMT\_MSA.3.1(a)** The TSF shall enforce the **Common Access Control SFP in Table 6-2**, [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

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

- None

[selection, choose one of: *restrictive, permissive, [assignment: other property]*]

- restrictive

**FMT\_MSA.3.2(a)** The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorized identified roles*]

- nobody

**FMT\_MSA.3(b) Static attribute initialisation**

**Hierarchical to:** No other components

**Dependencies:** FMT\_MSA.1 Management of security attributes

FMT\_SMR.1 Security roles

**FMT\_MSA.3.1(b)** The TSF shall enforce the **TOE Function Access Control Policy in Table 6-3**, [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

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

- None

[selection, choose one of: restrictive, permissive, [assignment: other property]]

- restrictive

**FMT\_MSA.3.2(b)** The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.

[assignment: *the authorized identified roles*]

- nobody

#### **FMT\_MTD.1 Management of TSF Data**

**Hierarchical to:** No other components

**Dependencies:** FMT\_SMR.1 Security roles

#### **FMT\_SMF.1 Specification of Management Functions**

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

[selection: *change\_default, query, modify, delete, clear, [assignment: other operations]*]

- See Table 6-9
- [assignment: other operations]

[assignment: *other operations*]

- See Table 6-9

[assignment: *list of TSF Data*]

- See Table 6-9

[selection, choose one of: *Nobody, [selection: U.ADMINISTRATOR, [assignment: the authorized identified roles except U.NORMAL]]*]

- See Table 6-9

**Table 6-9 Management of TSF Data**

| Category | TSF data                    | Operation                    | User role for which operation is permitted |
|----------|-----------------------------|------------------------------|--|
| D.PROT   | Administrator user ID       | [Selected operations] modify | Nobody                                     |
|          | Password policy             | [Selected operations] modify | U.ADMINISTRATOR                            |
|          | Non-operation timer setting | [Selected operations] modify | U.ADMINISTRATOR                            |

|        |   |                                 |                 |
|--------|---|---------------------------------|-----------------|
|        | Administrator authentication settings (operation panel)                   | [Selected operations] modify    | U.ADMINISTRATOR |
|        | User restriction settings   | [Selected operations] modify    | U.ADMINISTRATOR |
|        | IPsec settings  | [Selected operations] modify    | U.ADMINISTRATOR |
|        | Time settings   | [Selected operations] modify    | U.ADMINISTRATOR |
|        | Network settings  | [Selected operations] modify    | U.ADMINISTRATOR |
|        | Hash value for verifying integrity of firmware                            | [Selected operations] modify    | Nobody          |
| D.CONF | Administrator password  | [Selected operations] modify    | U.ADMINISTRATOR |
|        |   | [Selected operations] query     | Nobody          |
|        | Passwords to access external devices such as a mail server or file server | [Selected operations] modify    | U.ADMINISTRATOR |
|        |   | [Added operations] Newly create |                 |
|        |   | [Selected operations] query     | Nobody          |
|        | IPsec preshared key   | [Selected operations] modify    | U.ADMINISTRATOR |
|        |   | [Selected operations] query     | Nobody          |

**FMT\_MTD.1.1(b)** The TSF shall restrict the ability to [selection: *change\_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF Data associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL*] to [selection, choose one of: *Nobody, [selection: U.ADMINISTRATOR, the U.NORMAL to whom such TSF Data are associated]*].

[selection: *change\_default, query, modify, delete, clear, [assignment: other operations]*]

– See Table 6-10

– [assignment: other operations]

[assignment: *other operations*]

– See Table 6-10

[assignment: *list of TSF Data associated with a U.NORMAL or TSF Data associated with documents or jobs owned by a U.NORMAL*]

– See Table 6-10

[selection, choose one of: *Nobody, [selection: U.ADMINISTRATOR, the U.NORMAL to whom such TSF Data are associated]*]

– See Table 6-10

**Table 6-10 Management of TSF Data**

| Category | TSF data  | Operation                       | User role for which operation is permitted |
|----------|---|---------------------------------|--|
| D.PROT   | User ID of normal users                               | [Selected operations] delete    | U.ADMINISTRATOR                            |
|          |   | [Added operations] Newly create |  |
|          | List of recipients for scan/fax/email or address book | [Selected operations] delete    | U.ADMINISTRATOR                            |
|          |   | [Added operations] Newly create |  |
|          | Job status log  | [Selected operations] modify    | Nobody                                     |
| D.CONF   | Normal user passwords                                 | [Selected operations] delete    | U.ADMINISTRATOR                            |
|          |   | [Added operations] Newly create |  |
|          |   | [Selected operations] query     | Nobody                                     |

**FMT\_SMF.1 Specification of Management Functions****Hierarchical to:** No other components**Dependencies:** No dependencies

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

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

- See Table 6-11

**Table 6-11 Management Function List**

| Management Functionality  |
|---|
| Registration/deletion of user ID for normal users by U.ADMINISTRATOR  |
| Registration/deletion of list of recipients for scan/fax/email or address book by U.ADMINISTRATOR                   |
| Change of password policy by U.ADMINISTRATOR  |
| Change of non-operation timer settings by U.ADMINISTRATOR   |
| Change of administrator authentication settings (operation panel) by U.ADMINISTRATOR                                |
| Change of user restriction settings by U.ADMINISTRATOR  |
| Change of IPsec settings by U.ADMINISTRATOR   |
| Change of time settings by U.ADMINISTRATOR  |
| Change of network settings by U.ADMINISTRATOR   |
| Registration/deletion of user password for normal users by U.ADMINISTRATOR  |
| Change of administrator password by U.ADMINISTRATOR   |
| Registration/change of passwords to access external devices such as a mail server or file server by U.ADMINISTRATOR |
| Change of IPsec preshared key by U.ADMINISTRATOR  |

**FMT\_SMR.1 Security roles****Hierarchical to:** No other components**Dependencies:** FIA\_UID.1 Timing of identification

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

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

– Nobody

**FMT\_SMR.1.2** The TSF shall be able to associate users with roles, **except for the role “Nobody” to which no user shall be associated.**

## 6.1.5.Class FPT: Protection of the TSF

**FPT\_FDI\_EXP.1 Restricted forwarding of data to external interfaces****Hierarchical to:** No other components**Dependencies:** FMT\_SMF.1 Specification of Management Functions

FMT\_SMR.1 Security roles

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

**FPT\_STM.1 Reliable time stamps****Hierarchical to:** No other components**Dependencies:** No dependencies

**FPT\_STM.1.1** The TSF shall be able to provide reliable time stamps.

**FPT\_TST.1 TSF testing****Hierarchical to:** No other components**Dependencies:** No dependencies

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

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

– during initial start-up

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



- [assignment: parts of TSF]

[assignment: *parts of TSF*]

- Self-Test Function

**FPT\_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: *parts of TSF*], *TSF Data*].

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

- [assignment: parts of TSF]

[assignment: *parts of TSF*]

- Hash value for verifying integrity of firmware

**FPT\_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

#### 6.1.6.Class FTA: TOE access

**FTA\_SSL.3 TSF-initiated termination**

**Hierarchical to:** No other components

**Dependencies:** No dependencies

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

[assignment: *time interval of user inactivity*]

- See Table 6-12

**Table 6-12 User Inactive Time Interval**

| Action   | User inactive time interval  |
|--|--|
| Logon from the operation panel by an administrator | Set time in non-operation timer settings<br>(can be set by an administrator with a range from 10 seconds to 240 minutes) |
| Logon from the operation panel by a normal user    | Set time in non-operation timer settings<br>(can be set by an administrator with a range from 10 seconds to 240 minutes) |
| Logon from Web Config by an administrator          | 20 minutes   |

#### 6.1.7.Class FTP: Trusted paths/channels

**FTP\_ITC.1 Inter-TSF trusted channel**

**Hierarchical to:** No other components

**Dependencies:** No dependencies

- FTP\_ITC.1.1** The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
- FTP\_ITC.1.2** The TSF shall permit **the TSF, another trusted IT product** to initiate communication via the trusted channel.
- FTP\_ITC.1.3** The TSF shall initiate communication via the trusted channel for **communication of D.DOC, D.FUNC, D.PROT, and D.CONF over any Shared-medium Interface.**

## 6.2. Security Assurance Requirements

Table 6-13 lists the security assurance requirements for 2600.2-PP, Protection Profile for Hardcopy Devices, Operational Environment B, and related SFR packages, EAL 2 augmented by ALC\_FLR.2.

**Table 6-13 IEEE 2600.2 Security Assurance Requirements**

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

## 6.3. Security Requirements Rationale

This section describes the rationale behind security functional requirements, security assurance requirements,

and dependency analysis.

### 6.3.1. Security Functional Requirements rationale

Table 6-14 demonstrate the completeness of SFRs that fulfill the objectives of the TOE. Bold typeface items provide principal (P) fulfillment of the objectives, and normal typeface items provide supporting (S) fulfillment.

**Table 6-14 Completeness of Security Requirements**

|              | O.DOC.NO_DIS | O.DOC.NO_ALT | O.FUNC.NO_ALT | O.PROT.NO_ALT | O.CONF.NO_DIS | O.CONF.NO_ALT | O.USER.AUTHORIZED | O.INTERFACE.MANAGED | O.SOFTWARE.VERIFIED | O.AUDIT.LOGGED | O.AUDIT_STORAGE.PROTECTED | O.AUDIT_ACCESS.AUTHORIZED |
|--------------|--------------|--------------|---------------|---------------|---------------|---------------|-------------------|---------------------|---------------------|----------------|---------------------------|---------------------------|
| FAU_GEN.1    |              |              |               |               |               |               |                   |                     |                     | <b>P</b>       |                           |                           |
| FAU_GEN.2    |              |              |               |               |               |               |                   |                     |                     | <b>P</b>       |                           |                           |
| FAU_SAR.1    |              |              |               |               | <b>P</b>      |               |                   |                     |                     |                |                           | <b>P</b>                  |
| FAU_SAR.2    |              |              |               |               | <b>P</b>      |               |                   |                     |                     |                |                           | <b>P</b>                  |
| FAU_STG.1    |              |              |               |               |               | <b>P</b>      |                   |                     |                     |                | <b>P</b>                  |                           |
| FAU_STG.4    |              |              |               |               |               | <b>P</b>      |                   |                     |                     |                | <b>P</b>                  |                           |
| FDP_ACC.1(a) | <b>P</b>     | <b>P</b>     | <b>P</b>      |               |               |               |                   |                     |                     |                |                           |                           |
| FDP_ACC.1(b) |              |              |               |               |               |               | <b>P</b>          |                     |                     |                |                           |                           |
| FDP_ACF.1(a) | S            | S            | S             |               |               |               |                   |                     |                     |                |                           |                           |
| FDP_ACF.1(b) |              |              |               |               |               |               | S                 |                     |                     |                |                           |                           |
| FDP_RIP.1    | <b>P</b>     |              |               |               |               |               |                   |                     |                     |                |                           |                           |
| FIA_AFL.1    |              |              |               |               |               |               | S                 |                     |                     |                |                           |                           |
| FIA_ATD.1    |              |              |               |               |               |               | S                 |                     |                     |                |                           |                           |
| FIA_SOS.1    |              |              |               |               |               |               | S                 |                     |                     |                |                           |                           |
| FIA_UAU.1    |              |              |               |               |               |               | <b>P</b>          | <b>P</b>            |                     |                |                           |                           |
| FIA_UAU.7    |              |              |               |               |               |               | S                 |                     |                     |                |                           |                           |
| FIA_UID.1    | S            | S            | S             | S             | S             | S             | <b>P</b>          | <b>P</b>            |                     | S              |                           |                           |
| FIA_USB.1    |              |              |               |               |               |               | <b>P</b>          |                     |                     |                |                           |                           |
| FMT_MSA.1(a) | S            | S            | S             |               |               |               |                   |                     |                     |                |                           |                           |
| FMT_MSA.1(b) |              |              |               |               |               |               | S                 |                     |                     |                |                           |                           |
| FMT_MSA.3(a) | S            | S            | S             |               |               |               |                   |                     |                     |                |                           |                           |
| FMT_MSA.3(b) |              |              |               |               |               |               | S                 |                     |                     |                |                           |                           |

|               |   |   |   |   |   |   |   |   |   |   |  |  |
|---------------|---|---|---|---|---|---|---|---|---|---|--|--|
| FMT_MTD.1     |   |   |   | P | P | P |   |   |   |   |  |  |
| FMT_SMF.1     | S | S | S | S | S | S |   |   |   |   |  |  |
| FMT_SMR.1     | S | S | S | S | S | S | S |   |   |   |  |  |
| FPT_FDI_EXP.1 |   |   |   |   |   |   |   | P |   |   |  |  |
| FPT_STM.1     |   |   |   |   |   |   |   |   |   | S |  |  |
| FPT_TST.1     |   |   |   |   |   |   |   |   | P |   |  |  |
| FTA_SSL.3     |   |   |   |   |   |   | P | P |   |   |  |  |
| FTP_ITC.1     | P | P | P | P | P | P |   |   |   |   |  |  |

Table 6-15 shows the sufficiency of the SFR for achieving TOE objectives.

**Table 6-15 Sufficiency of Security Requirements**

| Objective  | SFR                 | Aim  |
|--|---------------------|--|
| O.DOC.NO_DIS<br>(Protection of D.DOC from unauthorized disclosure) | <b>FDP_ACC.1(a)</b> | <b>Establish access control objectives and implement protection</b>  |
|  | FDP_ACF.1(a)        | Provide access control functions and support access control objectives   |
|  | <b>FDP_RIP.1</b>    | <b>Make residual data unusable and implement protection</b>  |
|  | FIA_UID.1           | Demand user identification and support access control and security roles   |
|  | FMT_MSA.1(a)        | Manage security attributes and support access control functions  |
|  | FMT_MSA.3(a)        | Manage default security attributes and support access control functions  |
|  | FMT_SMF.1           | Demand attribute management functions and support security attribute management                                    |
|  | FMT_SMR.1           | Demand security roles and support security attribute management  |
|  | <b>FTP_ITC.1</b>    | <b>Demand the use of a trusted channel when communicating on a share media interface, and implement protection</b> |
| O.DOC.NO_ALT<br>(Protection of D.DOC from unauthorized alteration) | <b>FDP_ACC.1(a)</b> | <b>Establish access control objectives and implement protection</b>  |
|  | FDP_ACF.1(a)        | Provide access control functions and support access control objectives   |
|  | FIA_UID.1           | Demand user identification and support access control and security roles   |
|  | FMT_MSA.1(a)        | Manage security attributes and support access  |

|  |                     |  |
|--|---------------------|--|
|  |                     | control functions  |
|  | FMT_MSA.3(a)        | Manage default security attributes and support access control functions  |
|  | FMT_SMF.1           | Demand attribute management functions and support security attribute management                                    |
|  | FMT_SMR.1           | Demand security roles and support security attribute management  |
|  | <b>FTP_ITC.1</b>    | <b>Demand the use of a trusted channel when communicating on a share media interface, and implement protection</b> |
| O.FUNC.NO_ALT<br>(Protection of D.FUNC from unauthorized alteration) | <b>FDP_ACC.1(a)</b> | <b>Establish access control objectives and implement protection</b>  |
|  | FDP_ACF.1(b)        | Provide access control functions and support access control objectives   |
|  | FIA_UID.1           | Demand user identification and support access control and security roles   |
|  | FMT_MSA.1(a)        | Manage security attributes and support access control functions  |
|  | FMT_MSA.3(a)        | Manage default security attributes and support access control functions  |
|  | FMT_SMF.1           | Demand attribute management functions and support security attribute management                                    |
|  | FMT_SMR.1           | Demand security roles and support security attribute management  |
|  | <b>FTP_ITC.1</b>    | <b>Demand the use of a trusted channel when communicating on a share media interface, and implement protection</b> |
| O.PROT.NO_ALT<br>(Protection of D.PROT from unauthorized alteration) | FIA_UID.1           | Demand user identification and support access control and security roles   |
|  | <b>FMT_MTD.1</b>    | <b>Restrict access and implement protection</b>  |
|  | FMT_SMF.1           | Demand attribute management functions and support security attribute management                                    |
|  | FMT_SMR.1           | Demand security roles and support security attribute management  |
|  | <b>FTP_ITC.1</b>    | <b>Demand the use of a trusted channel when communicating on a share media interface, and implement protection</b> |
| O.CONF.NO_DIS  | <b>FAU_SAR.1</b>    | <b>Provide security audit records and</b>  |

|  |                     |  |
|--|---------------------|--|
| (Protection of D.CONF from unauthorized disclosure)  |                     | <b>implement audit objectives</b>  |
|  | <b>FAU_SAR.2</b>    | <b>Restrict the reading of security audit records and implement audit objectives</b>                               |
|  | FIA_UID.1           | Demand user identification and support access control and security roles   |
|  | <b>FMT_MTD.1</b>    | <b>Restrict access and implement protection</b>  |
|  | FMT_SMF.1           | Demand attribute management functions and support security attribute management                                    |
|  | FMT_SMR.1           | Demand security roles and support security attribute management  |
|  | <b>FTP_ITC.1</b>    | <b>Demand the use of a trusted channel when communicating on a share media interface, and implement protection</b> |
| O.CONF.NO_ALT<br>(Protection of D.CONF from unauthorized alteration)                           | <b>FAU_STG.1</b>    | <b>Protect from unauthorized deletion and modification, and implement auditing objectives</b>                      |
|  | <b>FAU_STG.4</b>    | <b>Prevent loss of audit data and implement auditing objectives</b>  |
|  | FIA_UID.1           | Demand user identification and support access control and security roles   |
|  | <b>FMT_MTD.1</b>    | <b>Restrict access and implement protection</b>  |
|  | FMT_SMF.1           | Demand attribute management functions and support security attribute management                                    |
|  | FMT_SMR.1           | Demand security roles and support security attribute management  |
|  | <b>FTP_ITC.1</b>    | <b>Demand the use of a trusted channel when communicating on a share media interface, and implement protection</b> |
| O.USER.AUTHORIZED<br>(Granting of permission for use of TOE to normal users and administrator) | <b>FDP_ACC.1(b)</b> | <b>Establish access control objectives and grant permissions</b>   |
|  | FDP_ACF.1(b)        | Provide access control functions and support access control objectives   |
|  | FIA_AFL.1           | Demand access control and grant permissions  |
|  | FIA_ATD.1           | Link security attributes to users and support granting of permissions  |
|  | FIA_SOS.1           | Demand confidential specifications and support granting of permissions   |
|  | <b>FIA_UAU.1</b>    | <b>Demand user authentication and grant</b>  |

|  |                      |   |
|--|----------------------|---|
|  |                      | <b>permissions</b>  |
|  | FIA_UAU.7            | Demand user authentication and grant permissions  |
|  | <b>FIA_UID.1</b>     | <b>Demand user identification and grant permissions</b>   |
|  | <b>FIA_USB.1</b>     | <b>Distinguish security attributes of subject linked to user role and grant permissions</b>   |
|  | FMT_MSA.1(b)         | Manage security attributes and support access control functions   |
|  | FMT_MSA.3(b)         | Manage default security attributes and support access control functions.  |
|  | FMT_SMR.1            | Demand security roles and support granting of permissions   |
|  | <b>FTA_SSL.3</b>     | <b>End a suspended session and grant permissions</b>  |
| O.INTERFACE.MANAGED<br>(external interface management)       | <b>FIA_UAU.1</b>     | <b>Demand user authentication and manage external interface</b>   |
|  | <b>FIA_UID.1</b>     | <b>Demand user authentication and manage external interface</b>   |
|  | <b>FPT_FDI_EXP.1</b> | <b>(As needed) demand an administrator to manage data transfer to a shared media interface from an external interface and manage external interface</b> |
|  | <b>FTA_SSL.3</b>     | <b>End a suspended session and manage external interface</b>  |
| O.SOFTWARE.VERIFIED<br>(software integrity verification)     | <b>FPT_TST.1</b>     | <b>Demand self-test and verify software</b>   |
| O.AUDIT.LOGGED<br>(record of auditable events)               | <b>FAU_GEN.1</b>     | <b>Demand logging of relevant events and implement auditing objectives</b>  |
|  | <b>FAU_GEN.2</b>     | <b>Demand logging of information linked to auditable events and implement auditing objectives</b>   |
|  | FIA_UID.1            | Link user identification to events and support auditing objectives  |
|  | FPT_STM.1            | Demand timestamps linked to events and support auditing objectives  |
| O. AUDIT_STORAGE.PROTECTED<br>(Protection of audit data from | <b>FAU_STG.1</b>     | <b>Protect from unauthorized deletion and modification, and implement auditing</b>  |

|   |                  |  |
|---|------------------|--|
| unauthorized access, deletion, and modification)                |                  | <b>objectives</b>  |
|   | <b>FAU_STG.4</b> | <b>Prevent loss of audit data and implement auditing objectives</b>                  |
| O. AUDIT_ACCESS.AUTHORIZED<br>(audit of security audit records) | <b>FAU_SAR.1</b> | <b>Provide security audit records and implement audit objectives</b>                 |
|   | <b>FAU_SAR.2</b> | <b>Restrict the reading of security audit records and implement audit objectives</b> |

### 6.3.2.Security Assurance Requirements rationale

This Security Target has been developed for Hardcopy Devices used in restrictive commercial information processing environments that require a relatively high level of document security, operational accountability, and information assurance. The TOE environment will be exposed to only a low level of risk because it is assumed that the TOE will be located in a restricted or monitored environment that provides almost constant protection from unauthorized and unmanaged access to the TOE and its data interfaces. Agents cannot physically access any nonvolatile storage without disassembling the TOE except for removable nonvolatile storage devices, where protection of User and TSF Data are provided when such devices are removed from the TOE environment. Agents have limited or no means of infiltrating the TOE with code to effect a change, and the TOE self-verifies its executable code to detect unintentional malfunctions. As such, the Evaluation Assurance Level 2 is appropriate.

EAL 2 is augmented with ALC\_FLR.2, Flaw reporting procedures. ALC\_FLR.2 ensures that instructions and procedures for the reporting and remediation of identified security flaws are in place, and their inclusion is expected by the consumers of this TOE.

### 6.3.3.Dependency Analysis

Table 6-16 shows the results of dependency analysis in this ST regarding TOE security function requirements.

**Table 6-16 Dependency Analysis Results for TOE Security Function Requirements**

| Function requirement | Dependency demanded in CC  | Dependency relation in this ST |
|----------------------|----------------------------|--------------------------------|
| FAU_GEN.1            | · FPT_STM.1                | · FPT_STM.1                    |
| FAU_GEN.2            | · FAU_GEN.1<br>· FIA_UID.1 | · FAU_GEN.1<br>· FIA_UID.1     |
| FAU_SAR.1            | · FAU_GEN.1                | · FAU_GEN.1                    |
| FAU_SAR.2            | · FAU_SAR.1                | · FAU_SAR.1                    |
| FAU_STG.1            | · FAU_GEN.1                | · FAU_GEN.1                    |
| FAU_STG.4            | · FAU_STG.1                | · FAU_STG.1                    |
| FDP_ACC.1(a)         | · FDP_ACF.1                | · FDP_ACF.1(a)                 |
| FDP_ACC.1(b)         | · FDP_ACF.1                | · FDP_ACF.1(b)                 |
| FDP_ACF.1(a)         | · FDP_ACC.1                | · FDP_ACC.1(a)                 |



|               |  |  |
|---------------|--|--|
|               | · FMT_MSA.3  | · FMT_MSA.3(a)                               |
| FDP_ACF.1(b)  | · FDP_ACC.1<br>· FMT_MSA.3                               | · FDP_ACC.1(b)<br>· FMT_MSA.3(b)             |
| FDP_RIP.1     | · None   | · None                                       |
| FIA_AFL.1     | · FIA_UAU.1  | · FIA_UAU.1                                  |
| FIA_ATD.1     | · None   | · None                                       |
| FIA_SOS.1     | · None   | · None                                       |
| FIA_UAU.1     | · FIA_UID.1  | · FIA_UID.1                                  |
| FIA_UAU.7     | · FIA_UAU.1  | · FIA_UAU.1                                  |
| FIA_UID.1     | · None   | · None                                       |
| FIA_USB.1     | · FIA_ATD.1  | · FIA_ATD.1                                  |
| FMT_MSA.1(a)  | · [FDP_ACC.1 or FDP_IFC.1]<br>· FMT_SMR.1<br>· FMT_SMF.1 | · FDP_ACC.1(a)<br>· FMT_SMR.1<br>· FMT_SMF.1 |
| FMT_MSA.1(b)  | · [FDP_ACC.1 or FDP_IFC.1]<br>· FMT_SMR.1<br>· FMT_SMF.1 | · FDP_ACC.1(b)<br>· FMT_SMR.1<br>· FMT_SMF.1 |
| FMT_MSA.3(a)  | · FMT_MSA.1<br>· FMT_SMR.1                               | · FMT_MSA.1(a)<br>· FMT_SMR.1                |
| FMT_MSA.3(b)  | · FMT_MSA.1<br>· FMT_SMR.1                               | · FMT_MSA.1(b)<br>· FMT_SMR.1                |
| FMT_MTD.1     | · FMT_SMR.1<br>· FMT_SMF.1                               | · FMT_SMR.1<br>· FMT_SMF.1                   |
| FMT_SMF.1     | · None   | · None                                       |
| FMT_SMR.1     | · FIA_UID.1  | · FIA_UID.1                                  |
| FPT_FDI_EXP.1 | · FMT_SMF.1<br>· FMT_SMR.1                               | · FMT_SMF.1<br>· FMT_SMR.1                   |
| FPT_STM.1     | · None   | · None                                       |
| FPT_TST.1     | · None   | · None                                       |
| FTA_SSL.3     | · None   | · None                                       |
| FTP_ITC.1     | · None   | · None                                       |

As above, all dependencies are fulfilled.

## 7. TOE Summary Specification

This section describes the TOE summary specification.

### 7.1. User Identification and Authentication Function

User identification and authentication functions refer to functions to identify and authenticate users of the TOE. The security function requirements for user identification and authentication are as below.

- FIA\_AFL.1, FIA\_ATD.1, FIA\_SOS.1, FIA\_UAU.1, FIA\_UAU.7, FIA\_UID.1, FIA\_USB.1, FTA\_SSL.3

#### (1) FIA\_AFL.1 Authentication failure handling

In the event of a failed login or authentication, the TOE locks the relevant account as per Table 7-1. Lockout are implemented for an individual interface rather than an individual user.

**Table 7-1 Action List Upon Authentication Failure**

| Logon or Authentication Pattern                            | Action upon unsuccessful authentication             |
|--|---|
| Logon from the operation panel by an administrator         | Lock the relevant administrator out for 0.6 seconds |
| Logon from the operation panel by a normal user            | Lock the relevant normal user out for 0.6 seconds   |
| Logon from Web Config by an administrator                  | Lock the relevant administrator out for 1 second    |
| Authentication upon receipt of a print job with a password | Lock the relevant normal user out for 1 second      |

#### (2) FIA\_ATD.1 User attribute definitions

The TOE defines and maintains user attributes as shown in Table 7-2.

**Table 7-2 Security Attribute List**

| User            | Security Attribute  |
|-----------------|---|
| U.NORMAL        | User ID of normal users<br>User role<br>Available Function List |
| U.ADMINISTRATOR | User role   |

#### (3) FIA\_SOS.1 Verification of secrets

The TOE verifies whether a password (password for normal user or administrator) conforms with a defined quality scale. The quality scale is as below.

- Length: 8 characters or more (maximum 20)
- Character types: must include at least one of the following character types
  - Upper-case letters
  - Lower-case letters
  - Numbers

· Symbols (!"#\$%&'()\*+,-./:;<=>?@[¥]^\_`{|}~ )

(4) FIA\_UAU.1 Timing of authentication

FIA\_UID.1 Timing of identification

The TOE verifies that the User ID and password of a normal user entered when the normal user logs in matches the User ID and password of the normal user registered in the TOE. The TOE verifies that a Password Print Job issued by a normal user matches the User ID and password of the normal user registered in the TOE. The TOE verifies that the User ID and password of an administrator entered when the administrator logs in matches the User ID and password of the administrator registered in the TOE. The TOE permits the following actions before normal user or administrator identification and authentication is implemented.

- Printer information display on operation panel
- Printer information print from operation panel
- Network information display on operation panel
- Network information print from operation panel
- Job list display on operation panel
- Help display on operation panel
- Printer information display on Web Config
- Network information display on Web Config
- Fax information display on operation panel
- Fax information print from operation panel
- Printer maintenance function execution from operation panel
- Printer status display on printer driver

(5) FIA\_UAU.7 Protected authentication feedback

The TOE displays the dummy characters shown in Table 7-3 on the logon screen when a password is entered upon logon from the operation panel or Web Config.

**Table 7-3 Dummy Characters during Password Input**

| Action   | Dummy character  |
|--|--|
| Logon from the operation panel by an administrator | * characters equaling the number of characters entered   |
| Logon from the operation panel by a normal user    | * characters equaling the number of characters entered   |
| Logon from Web Config by an administrator          | Mask characters equaling the number of characters entered<br>*Masked character types depend on the browser |

(6) FIA\_USB.1 User-subject binding

If user identification and authentication is successful, the TOE links the User ID of the normal user, user

role, and Available Function List user attributes to the subject as shown in Table 7-4.

**Table 7-4 Initial Linking Rules for Attributes**

| User          | Subject         | User Security Attribute   |
|---------------|-----------------|---|
| Normal user   | U.NORMAL        | User ID of normal users<br>User role<br>Available Function List |
| Administrator | U.ADMINISTRATOR | User role   |

(7) FTA\_SSL.3 TSF-initiated termination

The TOE performs automatic logoff if there is no operation from the operation panel or Web Config for a certain continuous period of time as shown in Table 7-5.

**Table 7-5 User Inactive Time Interval**

| Action   | User inactive time interval  |
|--|--|
| Logon from the operation panel by an administrator | Set time in non-operation timer settings<br>(can be set by an administrator with a range from 10 seconds to 240 minutes) |
| Logon from the operation panel by a normal user    | Set time in non-operation timer settings<br>(can be set by an administrator with a range from 10 seconds to 240 minutes) |
| Logon from Web Config by an administrator          | 20 minutes   |

## 7.2. Document Access Control Function

The document access control function is a function to restrict operations on user data. The security function requirements for the document access control function are as below.

- FDP\_ACC.1(a), FDP\_ACF.1(a), FMT\_MSA.3(a)

(1) FDP\_ACC.1(a) Subset access control

FDP\_ACF.1(a) Security attribute based access control

For D.DOC and D.FUNC generated by the basic functions in Table 7-6, the TOE follows access control rules for each user, and only permits access to data for permitted users.

**Table 7-6 Document Access Control Function Access Control Rules**

| Data            | Security Attribute  | Operation       | User        | Access control rule   |
|-----------------|---|-----------------|-------------|---|
| D.DOC<br>(+PRT) | User ID of normal users<br>Document data attributes<br>“+PRT” | Print<br>Delete | Normal user | For normal users, operation is only permitted for data that has the document data attribute “+PRT” and a normal user that matches the normal user User ID<br>– Printing is the operation of |

|              |   |   |               |  |
|--------------|---|---|---------------|--|
|              |   |   |               | print data being input from the printer driver and temporarily stored, and then output as a hard copy  |
|              |   | Delete  | Administrator | For an administrator, operation is only permitted for data with the document data attribute "+PRT"   |
| D.DOC (+SCN) | User ID of normal users<br>Document data attributes<br>"+SCN" | Email attachment sending<br>Sending to specified folder<br>Delete | Normal user   | For normal users, operation is only permitted for data that has the document data attribute "+SCN" and a normal user that matches the normal user User ID <ul style="list-style-type: none"> <li>Email attachment sending is an operation to attach a D.DOC to an email and send it, and it completes through a series of operations with scanning</li> <li>Specified folder sending is an operation to send D.DOC to a shared folder over a network, and it completes through a series of operations with scanning</li> </ul> |
|              |   | Email attachment sending<br>Sending to specified folder<br>Delete | Administrator | For an administrator, operation is only permitted for data with the document data attribute "+SCN"   |
| D.DOC (+CPY) | User ID of normal users<br>Document data attributes<br>"+CPY" | Copy print<br>Delete  | Normal user   | For normal users, operation is only permitted for data that has the document data attribute "+CPY" and a normal user that matches the normal user User ID <ul style="list-style-type: none"> <li>Copy print completes through a series of operations with</li> </ul>   |

|                   |                                      |   |               |  |
|-------------------|--------------------------------------|---|---------------|--|
|                   |                                      |   |               | scan and hardcopy output   |
|                   |                                      | Copy print<br>Delete  | Administrator | For an administrator, operation is only permitted for data with the document data attribute "+CPY"   |
| D.DOC<br>(+FAXIN) | Document data attributes<br>"+FAXIN" | Fax receiving and printing<br>Email attachment sending<br>Sending to specified folder<br>Fax forwarding<br>Preview display on operation panel<br>Delete | Normal user   | <p>For normal users, to which the fax receiving function (FAXIN) is assigned in the Available Function List, operation is only permitted for data that has the document data attribute "+FAXIN"</p> <ul style="list-style-type: none"> <li>– Email attachment sending is an operation to attach a D.DOC to an email and send it, and it completes through a series of operations with fax receiving</li> <li>– Specified folder sending is an operation to send D.DOC to a shared folder over a network, and it completes through a series of operations with fax receiving</li> <li>– Fax forwarding is an operation to transfer a D.DOC to a separate fax address, and it completes through a series of operations with fax receiving</li> <li>– Preview display on operation panel is an operation to display a D.DOC on the operation panel, and it completes through a series of operations with fax receiving</li> </ul> |
|                   |                                      | Fax receiving and printing<br>Email   | Administrator | For an administrator, operation is only permitted for data with the document data attribute "+FAXIN"   |

|                    |  |   |               |  |
|--------------------|--|---|---------------|--|
|                    |  | attachment<br>sending<br>Sending to<br>specified folder<br>Fax forwarding<br>Preview display<br>on operation<br>panel<br>Delete                           |               |  |
| D.DOC<br>(+FAXOUT) | User ID of normal<br>users<br>Document data<br>attributes<br>“+FAXOUT” | Fax sending<br>Preview display<br>on operation<br>panel<br>Delete   | Normal user   | For normal users, operation is only<br>permitted for data that has the<br>document data attribute<br>“+FAXOUT” and a normal user that<br>matches the normal user User ID<br>– Preview display on operation<br>panel is an operation to display<br>a D.DOC on the operation<br>panel, and it completes<br>through a series of operations<br>with fax sending  |
|                    |  | Fax sending<br>Preview display<br>on operation<br>panel<br>Delete   | Administrator | For an administrator, operation is<br>only permitted for data with the<br>document data attribute<br>“+FAXOUT”   |
| D.DOC<br>(+DSR)    | User ID of normal<br>users<br>Document data<br>attributes<br>“+DSR”    | Print document<br>stored in box<br>Preview display<br>on operation<br>panel<br>Email<br>attachment<br>sending<br>Sending to<br>specified folder<br>Delete | Normal user   | For normal users, operation is only<br>permitted for data that has the<br>document data attribute “+DSR”<br>and a normal user that matches the<br>normal user User ID<br>– Printing a document stored in<br>a box is the operation to output<br>a hard copy of a D.DOC stored<br>in a personal box<br>– Preview display on operation<br>panel is an operation to display<br>a D.DOC on the operation |

|                  |   |            |                              |   |
|------------------|---|------------|------------------------------|---|
|                  |   |            |                              | <p>panel</p> <ul style="list-style-type: none"> <li>– Email attachment sending is an operation to attach a D.DOC to an email and send it, and it completes through a series of operations with document storage and retrieval</li> <li>– Specified folder sending is an operation to send a D.DOC to a shared folder over a network, and it completes through a series of operations with document storage and retrieval</li> </ul> |
|                  |   | Delete     | Administrator                | For an administrator, operation is only permitted for data with the document data attribute “+DSR”  |
| D.FUNC<br>(+PRT) | User ID of normal users<br>Document data attributes<br>“+PRT” | Delete     | Normal user                  | For normal users, operation is only permitted for data that has the document data attribute “+PRT” and a normal user that matches the normal user User ID   |
|                  |   | Delete     | Administrator                | For an administrator, operation is only permitted for data with the document data attribute “+PRT”  |
|                  |   | Alteration | Normal user<br>Administrator | Operation not permitted   |
| D.FUNC<br>(+SCN) | User ID of normal users<br>Document data attributes<br>“+SCN” | Delete     | Normal user                  | For normal users, operation is only permitted for data that has the document data attribute “+SCN” and a normal user that matches the normal user User ID   |
|                  |   | Delete     | Administrator                | For an administrator, operation is only permitted for data with the document data attribute “+SCN”  |
|                  |   | Alteration | Normal user<br>Administrator | Operation not permitted   |



|                     |  |            |                              |  |
|---------------------|--|------------|------------------------------|--|
| D.FUNC<br>(+CPY)    | User ID of normal users<br>Document data attributes<br>“+CPY”    | Delete     | Normal user                  | For normal users, operation is only permitted for data that has the document data attribute “+CPY” and a normal user that matches the normal user User ID                                    |
|                     |  | Delete     | Administrator                | For an administrator, operation is only permitted for data with the document data attribute “+CPY”   |
|                     |  | Alteration | Normal user<br>Administrator | Operation not permitted  |
| D.FUNC<br>(+FAXIN)  | Document data attributes<br>“+FAXIN”                             | Delete     | Normal user                  | For normal users, to which the fax receiving function (FAXIN) is assigned in the Available Function List, operation is only permitted for data that has the document data attribute “+FAXIN” |
|                     |  | Delete     | Administrator                | For an administrator, operation is only permitted for data with the document data attribute “+FAXIN”   |
|                     |  | Alteration | Normal user<br>Administrator | Operation not permitted  |
| D.FUNC<br>(+FAXOUT) | User ID of normal users<br>Document data attributes<br>“+FAXOUT” | Delete     | Normal user                  | For normal users, operation is only permitted for data that has the document data attribute “+FAXOUT” and a normal user that matches the normal user User ID                                 |
|                     |  | Delete     | Administrator                | For an administrator, operation is only permitted for data with the document data attribute “+FAXOUT”  |
|                     |  | Alteration | Normal user<br>Administrator | Operation not permitted  |
| D.FUNC<br>(+DSR)    | User ID of normal users<br>Document data attributes<br>“+DSR”    | Delete     | Normal user                  | For normal users, operation is only permitted for data that has the document data attribute “+DSR” and a normal user that matches the normal user User ID                                    |
|                     |  | Delete     | Administrator                | For an administrator, operation is   |

|  |  |            |                              |   |
|--|--|------------|------------------------------|---|
|  |  |            |                              | only permitted for data with the document data attribute "+DSR" |
|  |  | Alteration | Normal user<br>Administrator | Operation not permitted   |

(2) FMT\_MSA.3(a) Static attribute initialisation

For D.DOC and D.FUNC that are newly generated in response to implemented MFP functions, the TOE configures the attributes shown in Table 7-7 as initial values.

**Table 7-7 Security Attribute Initial Values**

| Function  | Data             | Security Attribute Initial Value  |
|---|------------------|---|
| MFP function<br>(print)   | D.DOC (+PRT)     | "User ID for a normal user" of a normal user who created data                                       |
|   | D.FUNC (+PRT)    | Document data attributes (+PRT)   |
| MFP function<br>(scan)  | D.DOC (+SCN)     | User ID for a normal user of a normal user who created data   |
|   | D.FUNC (+SCN)    | *However, for administrator the identifier is "Administrator"<br>Document data attributes (+SCN)    |
| MFP function<br>(copy)  | D.DOC (+CPY)     | User ID for a normal user of a normal user who created data   |
|   | D.FUNC (+CPY)    | *However, for administrator the identifier is "Administrator"<br>Document data attributes (+CPY)    |
| MFP function<br>(fax receiving)                                     | D.DOC (+FAXIN)   | Document data attributes (+FAXIN)   |
|   | D.FUNC (+FAXIN)  |   |
| MFP function<br>(fax sending)                                       | D.DOC (+FAXOUT)  | User ID for a normal user of a normal user who created data   |
|   | D.FUNC (+FAXOUT) | *However, for administrator the identifier is "Administrator"<br>Document data attributes (+FAXOUT) |
| MFP function<br>(Document<br>Storage and<br>Retrieval<br>Functions) | D.DOC (+DSR)     | User ID for a normal user of a normal user who created data   |
|   | D.FUNC (+DSR)    | *However, for administrator the identifier is "Administrator"<br>Document data attributes (+DSR)    |

Note, the owner of documents related to fax receiving is a normal user to whom the Available Function List fax receiving function (FAXIN) has been granted by an administrator, and the owner of documents related to fax sending is a normal user to whom the Available Function List fax sending function (FAXOUT) has been granted by an administrator. Furthermore, the initial value of the security attributes shown in Table 7-7 are default values, and access is restricted by these security attributes meaning they are restrictive, and no function exists to define initial values that differ from the default values.

### 7.3. Access Control Function for TOE Function

The access control function for TOE functions is a function to restrict operation of TOE functions. The security

function requirements for the access control function for TOE functions are as below.

– FDP\_ACC.1(b), FDP\_ACF.1(b), FMT\_MSA.3(b)

(1) FDP\_ACC.1(b) Subset access control

FDP\_ACF.1(b) Security attribute based access control

For basic functions in Table 7-8, the TOE follows access control rules for each user, and only permits permitted users to execute jobs.

**Table 7-8 Access Control Rules of Access Control Function for TOE Functions**

| Function                | Operation                     | User          | Access control rule  |
|-------------------------|-------------------------------|---------------|--|
| MFP function<br>(print) | Job execution<br>Job deletion | Normal user   | For normal users to which the print (PRT) function is assigned in the Available Function List, operation is permitted  |
|                         | Job deletion                  | Administrator | For an administrator, operation is only permitted for functions with the function type “print”   |
| MFP function<br>(scan)  | Job execution<br>Job deletion | Normal user   | For normal users to which the scan (SCN) function is assigned in the Available Function List, operation is permitted   |
|                         | Job execution<br>Job deletion | Administrator | For an administrator, operation is only permitted for functions with the function type “scan attribute”  |
| MFP function<br>(copy)  | Job execution<br>Job deletion | Normal user   | For normal users to which the copy (CPY) function is assigned in the Available Function List, operation is permitted   |
|                         | Job execution<br>Job deletion | Administrator | For an administrator, operation is only permitted for functions with the function type “copy attribute”  |
| MFP function<br>(fax)   | Job execution<br>Job deletion | Normal user   | For normal users to which the fax receiving function (FAXIN) and fax sending function (FAXOUT) are assigned in the Available Function List, operation is permitted |
|                         | Job execution<br>Job deletion | Administrator | For an administrator, operation is only permitted for functions with the function type “fax attribute”   |
| MFP function            | Job execution                 | Normal user   | For normal users to which the  |

|                                  |                               |               |   |
|----------------------------------|-------------------------------|---------------|---|
| (document storage and retrieval) | Job deletion                  |               | document storage and retrieval (DSR) function is assigned in the Available Function List, operation is permitted                  |
|                                  | Job execution<br>Job deletion | Administrator | For an administrator, operation is only permitted for functions with the function type “document storage and retrieval attribute” |

(2) FMT\_MSA.3(b) Static attribute initialisation

For newly registered U.NORMAL, the TOE configures the Available Function List as the security attributes, but initial values disable use of all functions. The initial value of the security attributes are default values, and access is restricted by these security attributes meaning they are restrictive, and no function exists to define initial values that differ from the default values.

#### 7.4. Security Management Function

The security management function is a function to manage security functions. The security function requirements for security management functions are as below.

- FMT\_MSA.1(a), FMT\_MSA.1(b), FMT\_MTD.1, FMT\_SMF.1, FMT\_SMR.1

(1) FMT\_MSA.1(a) Management of security attributes

The TOE permits the following operations for administrator.

- Deletion, and new creation for User ID of normal users
- Available Function List modify

There are no roles that can modify the document data attributes and user roles.

(2) FMT\_MSA.1(b) Management of security attributes

The TOE permits the following operations for administrator.

- Available Function List modify

There are no roles that can modify the function type and user roles.

(3) FMT\_MTD.1 Management of TSF Data

The TOE only permits operations on TSF data by roles for which the operations in Table 7-9 are permitted.

**Table 7-9 Management of TSF Data**

| TSF data                | Operation            | User role for which operation is permitted |
|-------------------------|----------------------|--|
| User ID of normal users | delete, newly create | Administrator                              |
| Administrator user ID   | modify               | None                                       |

|   |                      |               |
|---|----------------------|---------------|
| List of recipients for scan/fax/email or address book                     | delete, newly create | Administrator |
| Job status log  | modify               | None          |
| Password policy   | modify               | Administrator |
| Non-operation timer setting   | modify               | Administrator |
| Administrator authentication settings (operation panel)                   | modify               | Administrator |
| User restriction settings   | modify               | Administrator |
| IPsec settings  | modify               | Administrator |
| Time settings   | modify               | Administrator |
| Network settings  | modify               | Administrator |
| Hash value for verifying integrity of firmware                            | modify               | None          |
| Normal user passwords   | delete, newly create | Administrator |
|   | query                | None          |
| Administrator password  | modify               | Administrator |
|   | query                | None          |
| Passwords to access external devices such as a mail server or file server | Newly create, modify | Administrator |
|   | query                | None          |
| IPsec preshared key   | modify               | Administrator |
|   | query                | None          |

#### (4) FMT\_SMF.1 Specification of Management Functions

The TOE provides the security management functions below.

**Table 7-10 Management Function List**

| Management Functionality  |
|---|
| Registration/deletion of user ID for normal users by U.ADMINISTRATOR                              |
| Registration/deletion of list of recipients for scan/fax/email or address book by U.ADMINISTRATOR |
| Change of password policy by U.ADMINISTRATOR  |
| Change of non-operation timer settings by U.ADMINISTRATOR   |
| Change of administrator authentication settings (operation panel) by U.ADMINISTRATOR              |
| Change of user restriction settings by U.ADMINISTRATOR  |
| Change of IPsec settings by U.ADMINISTRATOR   |
| Change of time settings by U.ADMINISTRATOR  |
| Change of network settings by U.ADMINISTRATOR   |
| Registration/deletion of U.NORMAL user password for normal users by U.ADMINISTRATOR               |

|   |
|---|
| Change of U.ADMINISTRATOR administrator password by U.ADMINISTRATOR   |
| Registration/change of passwords to access external devices such as a mail server or file server by U.ADMINISTRATOR |
| Change of IPsec preshared key by U.ADMINISTRATOR  |

(5) FMT\_SMR.1 Security roles

The TOE has the following roles, and links users to a role.

- Normal user
- Administrator

### 7.5. Residual Data Overwrite Function

The residual data overwrite function is a function to completely erase deleted or temporarily stored documents from an HDD or Flash ROM and make them unrecoverable. The security function requirements for the residual data overwrite function are as below.

- FDP\_RIP.1

(1) FDP\_RIP.1 Subset residual information protection

The TOE erases D.DOC saved on the HDD or Flash ROM after jobs performed by basic functions complete. The space used for D.DOC is sequentially overwritten with a specific value (0x00) to erase it. Overwriting to erase from the HDD is performed when the TOE starts up, and when residual data is discovered by the audit process. The TOE can also perform overwriting through manual operation from the operation panel.

### 7.6. Self-Test Function

The self test function is a function that verifies that part of the TSF operates normally and part of TSF data and TSF implementation code are complete when the MFP starts up. The security function requirements for the self test function are as below.

- FPT\_TST.1

(1) FPT\_TST.1 TSF test

The TOE performs the following self tests when the MFP starts up.

- It provides a function that calculates a hash value from the firmware file and checks that it matches the value stored in the TOE (a hash value to verifying integrity of the firmware), and by doing so verifies the integrity of part of the TSF data (firmware hash value) and the TSF implementation code as well as partially verifying the normal TSF operation

If an abnormality is detected in the self test, the TOE displays an error message on the MFP's operation panel and does not permit any subsequent operations.

## 7.7. Audit Log Function

The audit log function is a function that records TOE usage and security-related events as an audit log for reference. The security function requirements for the audit log function are as below.

- FAU\_GEN.1, FAU\_GEN.2, FAU\_SAR.1, FAU\_SAR.2, FAU\_STG.1, FAU\_STG.4, FPT\_STM.1

### (1) FAU\_GEN.1                      Audit data generation

If an auditable event shown in Table 7-11 occurs, the TOE creates audit data and records it as an audit log.

**Table 7-11 Auditable Events**

| Auditable Event                                   | Audit Data  | Additional information               |
|---|---|--------------------------------------|
| Audit log function start (success)                | <ul style="list-style-type: none"> <li>· Date of auditable event occurrence</li> <li>· Type of auditable event</li> <li>· Subject identification information of auditable event</li> <li>· Result of auditable event</li> </ul> | · None                               |
| Audit log function end (success)                  |   | · None                               |
| Use of authentication mechanism (success/failure) |   | · None                               |
| Use of identification mechanism (success/failure) |   | · None                               |
| Use of management functions (success/failure)     |   | · None                               |
| Change of time (success/failure)                  |   | · None                               |
| IPsec communication fail                          |   | · Communication recipient IP address |

The identification mechanism and authentication mechanism are unified, so if identification and authentication fail, there is no need to identify if it is an "identification-only failure". As such, user identification test is not applicable as additional information for the auditable event "use of identification mechanism (success/failure)".

### (2) FAU\_GEN.2                      User identity association

If an auditable event is brought about by a user's action, the TOE links the identification information of the user who caused it to the auditable event.

### (3) FAU\_SAR.1                      Audit review

The TOE permits administrator to read audit logs. The TOE also converts audit logs into a format the administrator can interpret. Administrator logons to Web Config to obtain audit logs (CSV format).

### (4) FAU\_SAR.2                      Restricted audit review

The TOE only permits administrator to read audit logs.

## (5) FAU\_STG.1 Protected audit trail storage

The TOE does not permit any user to edit audit logs. Also, the TOE permits only administrators to delete audit logs.

## (6) FAU\_STG.4 Prevention of audit data loss

When the audit logs are full, the TOE overwrites the audit logs starting with the oldest log.

## (7) FPT\_STM.1 Reliable time stamps

The TOE has an internal system clock. When an auditable event occurs, the date and time of the occurrence is recorded in the audit log using the system clock. The system clock obtains the time accurately from an NTP server, and it can also be synchronized.

### 7.8. Network Protection Function

The network protection function is a function to prevent information leakage and data tampering from the network due to eavesdropping when using the LAN. The security function requirements for the network protection function are as below.

– FPT\_FDI\_EXP.1, FTP\_ITC.1

## (1) FPT\_FDI\_EXP.1 Restricted information transfer to external interfaces

The TOE places fixed restrictions on wired LAN and telephone line information transfer as follows.

- The TOE does not directly transfer information input from a wired LAN to a telephone line without additional processing by TSF
- The TOE does not directly transfer information input from a telephone line to a wired LAN without additional processing by TSF

## (2) FTP\_ITC.1 Inter-TSF trusted channel

During communication between the MFP and servers/client PC, the TOE communicates using a trusted channel. The TOE provides IPsec encryption as a trusted channel. Table 7-12 shows the specifications regarding IPsec encrypted communication.

**Table 7-12 IPsec Specifications**

| Item                 | Details                      |
|----------------------|------------------------------|
| Encryption algorithm | AES(128bits,192bits,256bits) |