RICOH IM 460F/370F with Extended HDD Type M54
Security Target

Author: RICOH COMPANY, LTD.
Date: 2024-2-26
Version: 1.00

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

Table of Contents

List of Figures

List of Tables

1 ST Introduction

This section describes ST Reference, TOE Reference, TOE Overview and TOE Description.

1.1 ST Reference

The following is the identification information of this ST.

Title:

RICOH IM 460F/370F with Extended HDD Type M54 Security Target

Version: 1.00

Date: 2024-2-26

Author: RICOH COMPANY, LTD.

1.2 TOE Reference

The identification information of the TOE, whose TOE type is digital multifunction product (hereinafter "MFP"), is described below.

TOE Name: **RICOH IM 460F/370F with Extended HDD Type M54**

Version: J-1.00

The TOE consists of a combination of the target MFP on which software and hardware are installed and an optional product installed to configure the TOE.

The target MFPs described in Table 1 are products for Japanese domestic market, and are identified by the product name and model code.

Table 1 : Product Name and Model Code of the Target MFP

No.	Product Name	Model Code
1	RICOH IM 370F	D0DM-03
2	RICOH IM 460F	D0DN-00

The target optional product is described in Table 2, and is identified by the product name.

Table 2 : Product Names of the Optional Products

No.	Optional Product	Product Name
1	HDD	Extended HDD Type M54

Table 3 describes the combinations of the target MFP and the optional product that will be the TOE. The optional HDD must be installed on the target MFP.

Table 3 : Combinations of the Target MFP and Optional Product

No.	MFP		Optional Product
	Product Name	Model Code	Product Name
1	RICOH IM 370F	D0DM-03	Extended HDD Type M54
2	RICOH IM 460F	D0DN-00	Extended HDD Type M54

Table 4 describes the identification information of the software versions and part numbers installed in these MFPs. Software is identified by name, version, and part number. However, Keymicon, GraphicData, and LegacyUIData are identified by name and version.

Table 4: Version and Part Number of Software for Version J-1.00

No.	Name of Software for the MFP	Version	Part Number
1	CTL System	1.04	D0DM5550F
2	Printer	1.00	D0DM5551C
3	IRIPS PS3PDF	1.00	D0DM5553B
4	CheetahSystem	1.04	D0DN1420F
5	appsite	3.06.20	D0DN1441D
6	bleservice	1.00	D0DN1433B
7	camelsl	1.00	D0DN1452C
8	cispluginble	5.0.0	D0DN1446A
9	cispluginkeystr	1.00.00	D0DN1445A
10	cispluginnfc	1.00.00	D0DN1444A
11	devicemanagemen	1.01.00	D0DN1455D
12	ecoinfo	1.00	D0DN1432B
13	faxinfo	1.00	D0DN1430B
14	helpservice	1.00	D0DN1449B
15	iccd	1.01.00	D0DN1443A
16	introductionset	1.00	D0DN1448B
17	iwnnimelanguage	2.16.2	D0E01433

No.	Name of Software for the MFP	Version	Part Number
18	iwnnimelanguage	2.16.2	D0E01431
19	iwnnimelanguage	2.16.2	D0E01432
20	iwnnimeml	2.16.204	D0E01430C
21	kerberos	1.0	D0DN1451B
22	langswitcher	1.00	D0DN1428B
23	mediaappappui	1.00	D0DN1439C
24	mlpsmartdevicec	5.0.0	D0DN1427A
25	optimorurcmf	1.1.9	D0E01462C
26	programinfoserv	1.00	D0DN1434C
27	remotesupport	1.00	D0DN1453B
28	rsisetup	1.01.14	D0DN1456D
29	simpleauth	1.00.00	D0DN1426A
30	simpledirectcon	1.25	D0DN1447
31	simpleprinter	1.00	D0DN1435C
32	smartcopy	1.01	D0DN1436D
33	smartdocumentbo	1.00	D0DN1454C
34	smartfax	1.01	D0DN1438C
35	smartprtstoredj	1.00	D0DN1440C
36	smartscanner	1.01	D0DN1437D
37	smartscannerex	3.00	D0DN1450C
38	stopwidget	1.00	D0DN1431B
39	tonerstate	1.00	D0DN1429B
40	traywidget	1.00	D0DN1442B
41	Engine	1.04:06	D0DM5500D

No.	Name of Software for the Operation Panel	Version	Part Number
42	Firmware	1.04	D0DN1420F
43	Keymicon	1.08	No display
44	Bluetooth サービス	1.00	D0DN1433B

No.	Name of Software for the Operation Panel	Version	Part Number
45	Bluetooth 認証プラグイン	5.0.0	D0DN1446A
46	DeviceManagementService	1.01.00	D0DN1455D
47	GraphicData	0.10	DXXXXXXX
48	ICCardDispatcher	1.01.00	D0DN1443A
49	iWnn IME	2.16.204	D0E01430C
50	iWnn IME Korean Pack	2.16.2	D0E01433
51	iWnn IME Simplified Chinese Pack	2.16.2	D0E01431
52	iWnn IME Traditional Chinese Pack	2.16.2	D0E01432
53	KerberosService	1.0	D0DN1451B
54	LegacyUIData	0.24	DXXXXXXX
55	ProgramInfoService	1.00	D0DN1434C
56	RemoteSupportService	1.00	D0DN1453B
57	RicohScanGUIService	3.00	D0DN1450C
58	USB カードリーダー対応プラグイン	1.00.00	D0DN1445A
59	かんたんカード認証設定	1.00.00	D0DN1426A
60	かんたん文書印刷	1.00	D0DN1440C
61	アプリケーションサイト	3.06.20	D0DN1441D
62	カンタン入出力	5.0.0	D0DN1427A
63	クラウド設定	1.01.14	D0DN1456D
64	コピー	1.01	D0DN1436D
65	サポート設定	1.00	D0DN1449B
66	スキャナー	1.01	D0DN1437D
67	ストップウィジェット	1.00	D0DN1431B
68	ダイレクト接続	1.25	D0DN1447
69	トレイ設定/用紙残量	1.00	D0DN1442B
70	ドキュメントボックス	1.00	D0DN1454C
71	ファクス	1.01	D0DN1438C
72	プリンター情報確認	1.00	D0DN1435C
73	メディアプリント＆スキャン	1.00	D0DN1439C

No.	Name of Software for the Operation Panel	Version	Part Number
74	リモートコネクトサポート	1.1.9	D0E01462C
75	導入設定	1.00	D0DN1448B
76	操作部画面の遠隔操作	1.00	D0DN1452C
77	標準 IC カードプラグイン	1.00.00	D0DN1444A
78	言語切り替えｳｨｼﾞｪｯﾄ	1.00	D0DN1428B
79	ecoウィジェット	1.00	D0DN1432B
80	ｻﾌﾟﾗｲ残量表示ｳｨｼﾞｪｯﾄ	1.00	D0DN1429B
81	ﾌｧｸｽ受信文書ｳｨｼﾞｪｯﾄ	1.00	D0DN1430B

Make clear to the sales representative that you purchase the MFP as CC-certified product.

1.3 TOE Overview

This section defines TOE Type, and TOE Usage and Major Security Functions of the TOE.

1.3.1 TOE Type

This TOE is an MFP, which is an IT product that has Copy Function, Document Server Function, Printer Function, Scanner Function, and Fax Function.

1.3.2 TOE Usage and Major Security Functions of TOE

The TOE is an MFP which is assumed that it will be installed in an office and used in an environment where it is connected with a telephone line and the LAN as shown in Figure 1. The user uses each function (Copy Function, Document Server Function, Printer Function, Scanner Function, and Fax Function) by operating from the Operation Panel of the MFP or from the client computer connected by the LAN.

Security functions, such as Identification and Authentication, access control, Use-of-Feature Restriction, Stored Data Protection, Residual Data Overwrite, and encrypted communication functions, are provided to prevent disclosure or alteration of assets, including document data processed by the TOE and setting information related to security functions, through unauthorised access to the TOE or communication data on the network. The TOE also provides a function to prevent unauthorised intrusion from telephone lines to the LAN. Events occurred on the TOE can be confirmed by the MFP administrator as audit log, and the MFP administrator can use the management functions from the Operation Panel or the client computer. In addition, the TOE verifies the integrity of the software configuration.

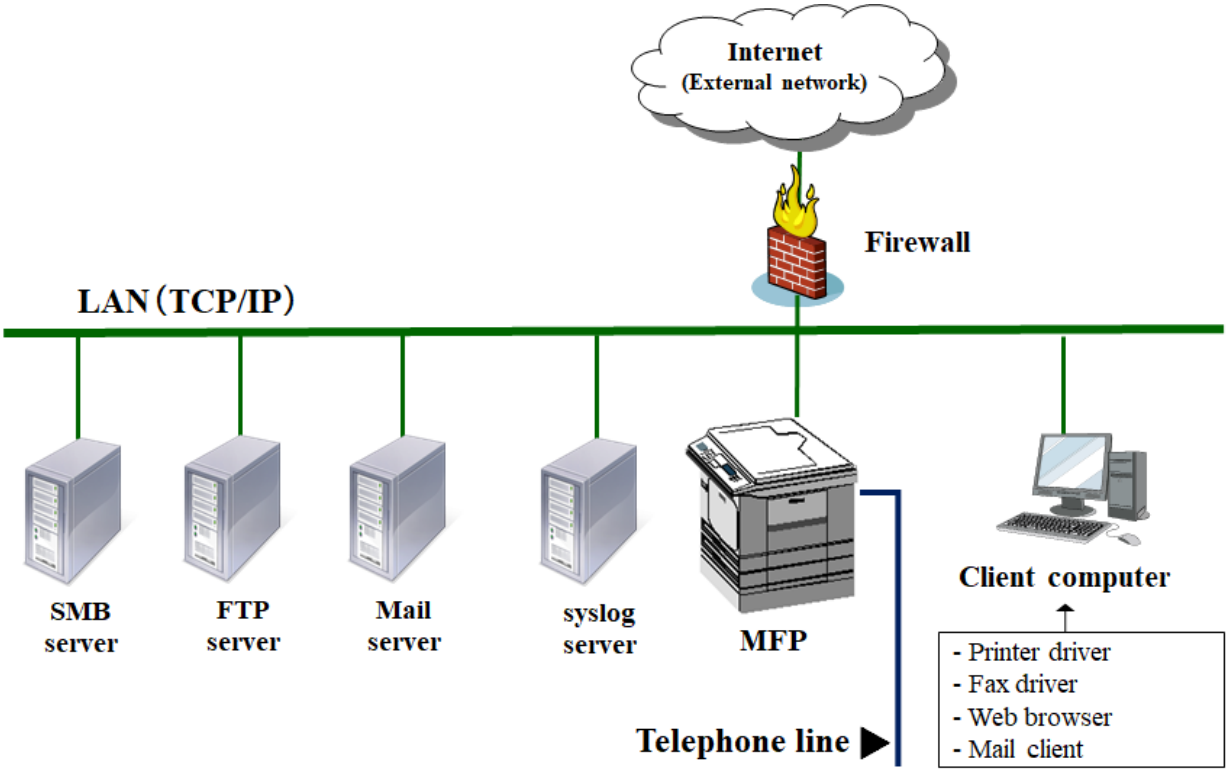


Figure 1 : Example of TOE Environment

1.3.3 Hardware and Software Other than TOE That Is Necessary for the TOE

The following describes components other than TOE in the operational environment illustrated in Figure 1.

- Client computer
  - By connecting to the LAN, a computer performs as a client of the TOE and users can remotely operate the MFP from the client computer. It is necessary to use a Web browser to operate various MFP settings and user data from the client computer. In order to temporarily save or store document data from the client computer, it is necessary to install the printer driver called RPCS Driver (1.0.0.0 and later versions) provided by RICOH, which has a function that supports TLS (IPP over SSL). In addition, in order to store document data for fax transmission from the client computer, it is necessary to install the fax driver called PC FAX Generic Driver (13.1.0.0 and later versions) provided by RICOH, which has a function that supports TLS (IPP over SSL). For the client computer that receives e-mail, it is necessary to install a mail client that supports S/MIME.
- SMB server

- A server that is used to send document data scanned by the Scanner Function of the TOE using the SMB protocol. The communication is protected by IPsec. It is necessary to use the folder transmission function.

- FTP server
  - A server that is used to send document data scanned by the Scanner Function of the TOE using the FTP protocol. The communication is protected by IPsec. It is necessary to use the folder transmission function.
- Mail server
  - A server that is used when the TOE sends e-mail. The server supports the SMTP protocol. It is necessary to use the e-mail transmission of attachments function.
- syslog server
  - A server that can receive the audit log recorded by the TOE. The server uses the syslog protocol and has a TLS-enabled service installed. The audit log can be transferred to the syslog server as well. If the transfer setting is enabled, this server is used as a destination of the audit log.

The TOE is connected to the LAN to use the network, and connected to the telephone line to send and receive data to and from external faxes. In order to connect the TOE to an external network, it is necessary to set up a firewall to protect the TOE from unauthorised access from the external network.

Hardware and software other than TOE that was used in the TOE evaluation are shown below.

- Client computer
  - OS: Windows 10 and Windows 11
  - Printer driver: RPCS Driver 1.0.0.0
  - Fax driver: PC FAX Generic Driver 13.1.0.0
  - Web browser: Microsoft Edge 107
  - Mail client: Thunderbird 102.6.0
- SMB server: Windows 10
- FTP server: Windows 10 (IIS10) version V10.0.19041.804
  Linux (Ubuntu 20.04) vsftpd 3.0.3
- Mail server: Windows 10 P-Mail Server Manager version 1.91
- syslog server: Linux (Ubuntu 20.04) rsyslogd 8.2001.0

1.4 TOE Description

This section describes the physical boundary and the logical boundary of the TOE.

1.4.1 Physical Boundary of TOE

The TOE consists of the MFP products in Table 1, the optional product in Table 2, and guidance documents inTable 6.

The MFP product is the MFP on which the software that configures the versions (J-1.00) described in Table 5 is installed. "Extended HDD Type M54" is the hardware of HDD, and must be installed on all MFPs.

A delivery company delivers the MFP and the optional product to users. Some guidance documents are included in the MFP product, and others are delivered through the Web.

Guidance documents will be delivered to users in the combinations described below.

Table 5 : Combinations to be Delivered

No.	MFP			Optional Product		Guidance Document	Remarks
	Product Name	Model Code	Version	Product Name	Version		
1	RICOH IM 370F	D0DM-03	J-1.00	Extended HDD Type M54	N/A	See Table 6.	SPDF is installed as standard
2	RICOH IM 460F	D0DN-00	J-1.00	Extended HDD Type M54	N/A	See Table 6.	SPDF is installed as standard

Table 6 describes guidance documents, formats, and delivery methods for the TOE.

Table 6: Guidance Documents

No.	Part Number	Guidance Document Name	Format	Delivery Method
1	D0DM-7002	かんたん操作ガイド	Brochure	Included in the product
2	D0DM-7013	本機を安全にご利用いただくために	Brochure	Included in the product
3	D0DM-7300	安全上のご注意	PDF	Through the Web
4	D0DM7302	使用説明書 RICOH IM 460F/370F	HTML	Through the Web
5	D0E37515	セキュリティーリファレンス	HTML	Through the Web
6	D0DM-7306 2024.02.08	使用説明書〈IEEE Std 2600.2™-2009 準拠でお使いになる管理者の方へ〉	PDF	Through the Web
7	D0E3-7510 2023.09.28	セキュリティー機能をお使いになるお客様へ	PDF	Through the Web
8	83NHEZ-JAR1.00 v281	ヘルプ	HTML	Through the Web

Guidance documents to be delivered through the Web can be downloaded from the following URL.

https://support.ricoh.com/services/device/ccmanual/IM_460_370-2600-spf/ja/Guidance_ja.zip

Hash value (SHA256): 49c9198b883cf9ffb0b84e35920f3b8cbfc6ed6f784a6fceb5e13b7b0fdeb597

1.4.2 Logical Boundary of TOE

The logical boundary of the TOE is described below.

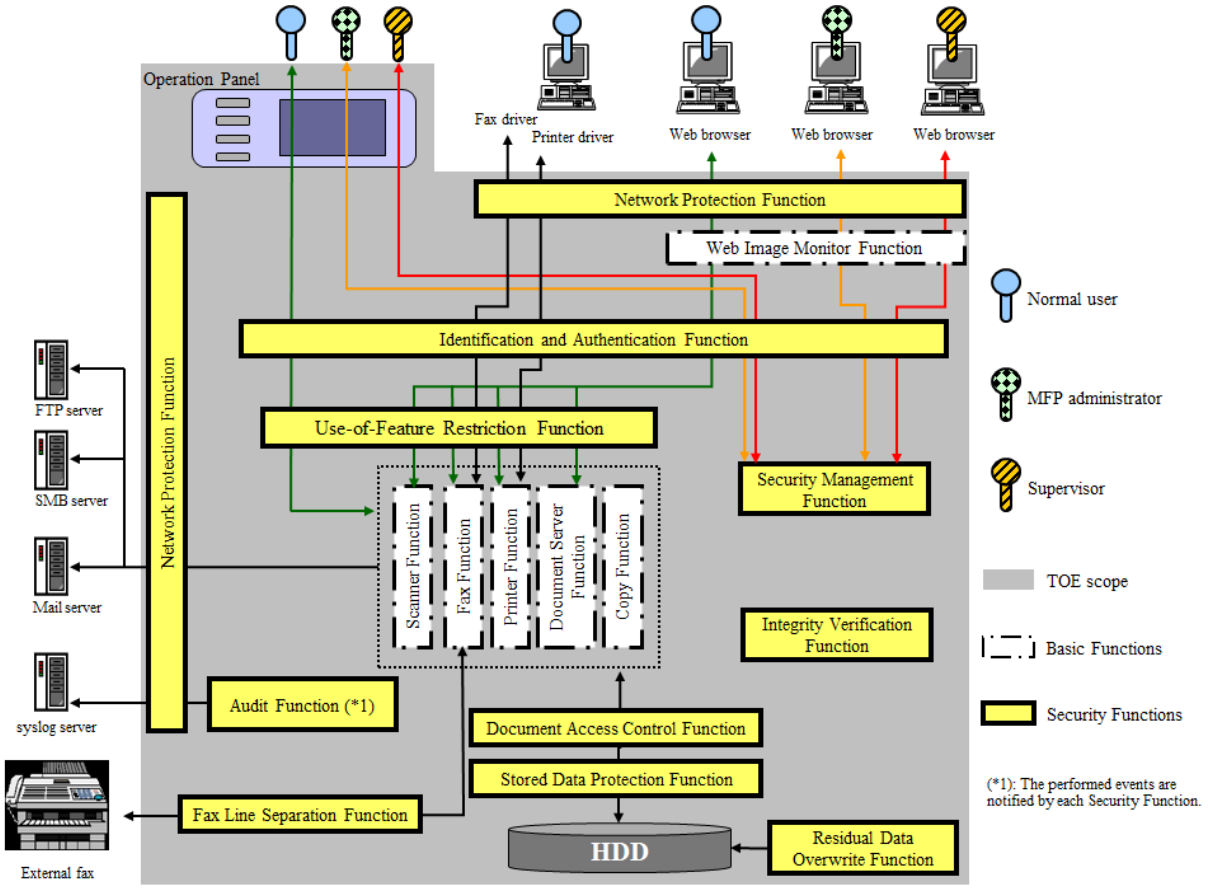


Figure 2: Logical Boundary of the TOE

1.4.2.1. Basic Functions

The overview of the Basic Functions is described as follows. The Copy Function, Printer Function, Scanner Function, Fax Function, and Document Server Function are MFP applications of the TOE, and the PP SFR Package function that each function has is shown in parentheses.

Copy Function

The Copy Function has a function to scan a paper document and then copy and print the scanned image data from the Operation Panel (F.CPY). Also, image to be copied and printed can be stored in the TOE (F.SCN and F.DSR). The document data stored at this time can be operated as a Document Server document from the Operation Panel or Web browser by using the Document Server Function.

Printer Function

The Printer Function temporarily saves the document data received from the printer driver by specifying a print method that is handled as temporary saving in the TOE. The document data is then printed, previewed, or deleted from the Operation Panel, or deleted from the Web browser as a temporary saved document (F.PRT).

When the print method is specified as stored print in the printer driver, the document data received by the TOE from the printer driver can be stored in the TOE, and the stored document data can be printed, previewed, or deleted from the Operation Panel, or can be deleted from the Web browser as a stored print document (F.DSR. F.DSR and F.PRT only for printing).

When the print method is specified as Document Server storage in the printer driver, the document data can be stored in the TOE from the printer driver (F.DSR). The document data stored at this time can be operated as a Document Server document from the Operation Panel or Web browser by using the Document Server Function.

Scanner Function

The Scanner Function has a function to scan a paper document and then send the scanned image data to FTP server or SMB server by using folder transmission, and to the mail server by using e-mail transmission of attachments from the Operation Panel. The data can also be previewed on the Operation Panel before sending (F.SCN).

The scanned image of the paper document from the Operation Panel can be stored in the TOE (F.SCN and F.DSR). The stored document data can be sent by using the folder transmission or e-mail transmission of attachments functions, previewed, or deleted as a scanned document from the Operation Panel (F.DSR). The document data stored at this time can also be operated as a scanned document from the Web browser by using the Document Server Function.

Fax Function

The Fax Function consists of Fax Transmission Function and Fax Reception Function. The fax compliant with the G3 standard, which uses a telephone line, is the target of evaluation.

The Fax Transmission Function has a function to send scanned image of paper documents as document data to external fax devices from the Operation Panel. The data can also be previewed on the Operation Panel before sending (F.FAX).

Also, the scanned image of paper documents from the Operation Panel can be stored in the TOE (F.SCN and F.DSR), or the received document data from the fax driver can be stored in the TOE. The stored document data can be sent by fax transmission, previewed, or deleted as a fax transmission document from the Operation Panel (F.DSR). The document data stored at this time can also be operated as a fax transmission document from the Operation Panel or Web browser by using the Document Server Function.

The Fax Reception Function has a function to receive document data from external fax devices via a telephone line (F.FAX), and then store it in the TOE (F.DSR). The stored document data can be printed, previewed, or deleted as a fax reception document from the Operation Panel, or can be downloaded, previewed, or deleted from the Web browser (F.DSR. F.DSR and F.PRT only for printing).

Document Server Function

The Document Server Function stores the scanned image of paper documents in the TOE from the Operation Panel (F.SCN and F.DSR). As a Document Server document, the stored document data is printed, previewed, or deleted from the Operation Panel, or previewed or deleted from the Web browser (F.DSR. F.DSR and F.PRT only for printing).

The document data stored by other functions also can be operated. (F.DSR for all. F.DSR and F.PRT only for printing). Those document data and operations are shown below.

- Document Server documents (stored by the Copy Function or Printer Function) can be printed, previewed, or deleted from the Operation Panel, or previewed or deleted from the Web browser.
- Fax transmission documents can be printed, previewed, or deleted from the Operation Panel, or can be sent by fax transmission, downloaded, previewed, or deleted from the Web browser.
- Scanned documents can be sent by using folder transmission or e-mail transmission of attachments functions, downloaded, previewed, or deleted from the Web browser.

Web Image Monitor Function

The Web Image Monitor Function is a function for the TOE user to remotely control the TOE from the Web browser. It is sometimes referred to as "WIM".

1.4.2.2. Security Function

The Security Functions are described as follows.

Audit Function

The Audit Function is to record a log that associates TOE use events and security-relevant events (hereinafter, "audit events") with user identification information as the audit log. Also, this function provides the recorded audit log in a format that can be audited. The recorded audit log can be downloaded and deleted only by the MFP administrator.

The date and time to be recorded in the audit log are derived from the system clock of the TOE. The oldest audit log is overwritten with the newest audit log when there is insufficient space in the audit log files to append the newest audit log. The TOE can transfer the audit log to the syslog server.

Identification and Authentication Function

The Identification and Authentication Function is to verify whether a person who attempts to use the TOE is an authorised user by performing identification and authentication with login user name and login password, so that the TOE can allow only the authenticated users to operate the management functions and the MFP applications. This function includes the following functionality:

- Authentication feedback area protection function that displays a login password using dummy letters when entering the login password
- Lockout function that prohibits users from logging in when the number of consecutive authentication failures reaches the threshold

- A function for protection of the quality of login passwords that registers only passwords satisfying the conditions of the minimum character number of passwords and the required character type defined in advance by the MFP administrator
- A function for automatic user logout when no operation is performed for a certain period of time from the logged-in state

Document Access Control Function

The Document Access Control Function is to authorise the operations for document data and user job data by the authorised TOE users who are authenticated by the Identification and Authentication Function. It allows user's operation on the document data and user job data based on the privileges for the user role, or the operation permissions for each user.

Use-of-Feature Restriction Function

The Use-of-Feature Restriction Function is to authorise the job execution of the MFP applications by the authorised TOE users who are authenticated by the Identification and Authentication Function based on the user role and the operation permissions for each user.

Network Protection Function

The Network Protection Function is to prevent information leakage due to network monitoring and detect alteration of communication details by providing encrypted communication when communicating with trusted IT products. Communication with the client computer when using WIM, printer driver, or fax driver is encrypted by TLS, and communication with SMB server and FTP server when using folder transmission is protected by IPsec. Also, communication with mail server when using e-mail transmission of attachments is protected by S/MIME, and communication with syslog server when the audit log transfer setting is enabled is encrypted by TLS.

Residual Data Overwrite Function

The Residual Data Overwrite Function is to overwrite random numbers or specific pattern data on the HDD and disable the reusing of the residual data included in deleted document data, temporary document data and their fragments on the HDD.

Security Management Function

The Security Management Function is to control operations for TSF data in accordance with user privileges allocated to each user or user role privileges allocated to the normal user, MFP administrator, and supervisor. In order to enable control, this function includes a function to maintain the user role of operating the Security Management Function and associate the user role with the authorised TOE user authenticated by the Identification and Authentication Function, and a function to set appropriate default values for the security attributes.

Integrity Verification Function

The Integrity Verification Function is a self-test function to verify that a part of TSF and the TSF executable code have a software configuration that maintains integrity during the MFP initial start-up.

Fax Line Separation Function

The Fax Line Separation Function is to restrict the input information from the telephone line to the LAN to only fax reception and prohibit forwarding of received faxes in order to prevent unauthorised intrusion into the LAN from the telephone line (same meaning as Fax Line in this function name).

Stored Data Protection Function

The Stored Data Protection Function is to encrypt data to be written to the HDD in order to protect data recorded in the HDD from data leakage.

2 Conformance Claim

This section describes Conformance Claims.

2.1 CC Conformance Claim

The CC conformance claim of this ST and TOE is as follows:

- CC version for which this ST and TOE claim conformance

  Part 1:

  Introduction and general model April 2017 Version 3.1 Revision 5 (Japanese translation ver.1.0) CCMB-2017-04-001

  Part 2:

  Security functional components April 2017 Version 3.1 Revision 5 (Japanese translation ver.1.0) CCMB-2017-04-002

  Part 3:

  Security assurance components April 2017 Version 3.1 Revision 5 (Japanese translation ver.1.0) CCMB-2017-04-003

- Functional requirements: Part 2 extended
- Assurance requirements: Part 3 conformance

2.2 PP Claims

The PP to which this ST and TOE are demonstrable conformant is:

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

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

2.3 Package Claims

The package conformance claims of this ST are described below.

This ST and TOE claim augmentation of package: EAL2, and augment assurance components of ALC_FLR.2. It conforms to the package names described in the Package Reference below.

Table 7 : Package Reference

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

2.4 Conformance Claim Rationale

2.4.1 Consistency Claim with TOE Type in PP

The product type targeted by the PP is the Hardcopy devices (hereinafter, HCDs). The HCDs consist of the scanner device and print device, and have the interface to connect telephone line. The HCDs combine these devices and equip one or more functions of Printer (F.PRT), Scanner (F.SCN), Copy (F.CPY), or Fax (F.FAX) Function. Some HCDs have a non-volatile memory medium such as hard disk drive and the Document Server Function (F.DSR). The type of this TOE is MFP. As an MFP, the TOE equips a non-volatile memory medium, interface for connecting telephone line, scanner device, and print device, and has the Copy, Scanner, Printer, Fax, and Document Server Functions. These allow printing (F.PRT), scanning (F.SCN), copying (F.CPY), faxing (F.FAX), and saving/retrieving documents (F.DSR). It can be said that MFP (the type of this TOE) has the characteristics of HCDs and is consistent with the TOE type of the PP.

2.4.2 Consistency Claim with Security Problems and Security Objectives in PP

Security Problem Definitions in section 3 of this ST defines all security problems of the PP and also P.STORAGE.ENCRYPTION is augmented, and Security Objectives in section 4 of this ST defines all security objectives of the PP and also O.STORAGE.ENCRYPTED is augmented. Described below are the rationale for the augmented security problems and security objectives that conform to the PP.

Although the PP is written in English, Security Problem Definitions in section 3 and Security Objectives in section 4 are translated from English into Japanese. When translating into Japanese, not all PP translation was literal, and some expressions were made comprehensible. This, however, does not mean that its description deviates from the requirements of the PP conformance.

For those points mentioned above, the security problems and security objectives in this ST are consistent with those in the PP.

Augmentation of P.STORAGE.ENCRYPTION and O.STORAGE.ENCRYPTED

P.STORAGE.ENCRYPTION and O.STORAGE.ENCRYPTED are for encrypting data on the HDD, and satisfy both other organisational security policies included in the PP and the security objectives of the TOE. Therefore, it conforms to the PP although P.STORAGE.ENCRYPTION and O.STORAGE.ENCRYPTED are augmented.

2.4.3 Consistency Claim with Security Requirements in PP

The SARs of this TOE are consistent with the PP as no augmentation or deletion has been made for the contents of the PP.

The SFRs for this TOE consist of the Common Security Functional Requirements, 2600.2-PRT, 2600.2-SCN, 2600.2-CPY, 2600.2-FAX, 2600.2-DSR, and 2600.2-SMI. The Common Security Functional Requirements are the indispensable SFR specified by the PP. 2600.2-PRT, 2600.2-SCN, 2600.2-CPY, 2600.2-FAX, 2600.2-DSR, and 2600.2-SMI are selected from the SFR Package specified by the PP. 2600.2-NVS is not selected because this TOE does not have any non-volatile memory medium that is detachable.

Although the security requirements of this ST were partly augmented and instantiated over the security requirements of the PP, they are still consistent with the PP. Described below are the parts augmented and instantiated with the reasons for their consistency with the PP.

Augmentation of FAU_STG.1, FAU_STG.4, FAU_SAR.1, and FAU_SAR.2

FAU_STG.1, FAU_STG.4, FAU_SAR.1, and FAU_SAR.2 are augmented according to PP APPLICATION NOTE 7 in order for this TOE to maintain and manage the audit logs.

Augmentation of FIA_AFL.1, FIA_UAU.7, and FIA_SOS.1

For the Identification and Authentication Function, this TOE augments FIA_AFL.1, FIA_UAU.7, and FIA_SOS.1 according to PP APPLICATION NOTE 38.

Augmentation of FCS_CKM.1, FCS_CKM.4, and FCS_COP.1

This TOE claims O.STORAGE.ENCRYPTED as a security objective of data protection for non-volatile memory media that administrators is not allowed to detach. To fulfill this, the functional requirements of FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 are augmented.

By this augmentation, the TOE behaviours are more restricted than by the PP. This augmentation is more restrictive than the security requirements of the PP, because all TOEs that satisfy this ST also satisfy the PP without mitigating other requirements. Therefore, it conforms to the PP although FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 are augmented.

Augmentation of FMT_MOF.1

This TOE satisfies the common security requirements in the PP for O.PROT.NO_ALT, and also augments FMT_MOF.1 that restricts the operation and suspension of management functions related to audit log settings to the MFP administrator. This augmentation is more restrictive than the requirements in the PP, because all TOEs that satisfy this ST also satisfy the PP without mitigating other requirements. Therefore, it conforms to the PP although FMT_MOF.1 is augmented.

Consistency Claim of FAU_GEN.1

For auditable events related to FMT_SMR.1, although it is described as "Modifications to the group of users that are part of a role" in the audit information required in the PP, it is described as "No record because there is no function for modifications to the group of users" in this TOE. This is because user roles of this TOE cannot be changed to other roles. This is not an auditable event, and it can be said that it conforms to the PP. Regarding other auditable events, this TOE covers more auditable events than that required or recommended by the PP, but these are augmented while the audit information and levels required or recommended by the PP are satisfied, so it can be said that it conforms to the PP.

Administrator Classification

In this ST, U.ADMINISTRATOR is classified into MFP administrator and supervisor. The administrator classification is made to the extent that none of the roles deviates from the definition of U.ADMINISTRATOR in the PP as a user who is specifically allowed to manage the entire TOE or a part of it and whose actions affect the TOE security policy, so it can be said that it conforms to the PP.

Consistency Rationale of FDP_ACF.1(a)

In FDP_ACF.1(a), this ST also describes the access control rule for +CPY document data. CPY SFR Package in the PP does not require access control, but this access control rule is more restrictive in accordance with PP APPLICATION NOTE 88, so it can be said that it conforms to the PP.

Therefore, FDP_ACF.1(a) in this ST satisfies FDP_ACF.1(a) in the PP.

3 Security Problem Definitions

This section describes Users, Assets, Threats, Organisational Security Policies, and Assumptions.

3.1 Definition of Users

This section defines the users related to the TOE.

The users consist of normal users and administrators, and the administrator are divided into the MFP administrator and the supervisor.

As described in Table 8, the users are classified according to their respective roles, and have privileges based on the roles of normal users, MFP administrators, and a supervisor.

Table 8 : Definition of Users

Definition of Users			Explanation
User (U.USER)	Normal user (U.NORMAL)		A user who is allowed to use the TOE. A normal user is provided with a login user name, and can use the MFP applications.
	Administrator (U.ADMINISTRATOR)	MFP administrator	A user who has the privilege to manage the TOE, including: - Operation of configuration of normal user settings - Operation of setting information related to MFP device behaviour - Operation of audit logs - Operation of configuration of network settings - Access management of fax reception document - Unlocking locked-out normal users and a supervisor
		Supervisor	A user who has the privilege to manage the TOE, including: - Changing login password of MFP administrators - Unlocking locked-out MFP administrators

3.2 Assets

Assets to be protected by the TOE are user data, TSF data, and functions. Table 9 describes the definitions.

Table 9 : Asset Categories

Category	Definition
User data	Data for the user created by the user, that does not affect the operation of the TSF.
TSF data	Data for the TOE created by the TOE, that may affect the operation of the TSF.
Functions	The MFP applications provided by the TOE to print (F.PRT), scan (F.SCN), copy (F.CPY), fax (F.FAX), and save and retrieve documents (F.DSR) to operate the user data.

3.2.1 User Data

The user data is categorized into document data and user job data. Table 10 defines categories.

Table 10 : Definitions of User Data

Category	Definition
Document data (D.DOC)	Paper documents, digitised documents, deleted documents, temporary documents, or their fragments managed by the TOE.
User job data (D.FUNC)	Information related to the user's document or document processing job.

3.2.2 TSF Data

The TSF data is categorized into TSF protected data and TSF confidential data. Table 11 defines categories.

Table 11 : TSF Data Categories

Category	Definition
TSF protected data (D.PROT)	This data must be protected from modifications by unauthorised persons. No security threat will occur even this data is exposed to the public.
TSF confidential data (D.CONF)	This data must be protected from modifications by unauthorised persons and reading by users without viewing permissions.

The TSF data handled by this TOE for each category are shown below.

Table 12 : Definitions of TSF Data

Category	TSF Data	Description
TSF protected data (D.PROT)	Lockout settings	Settings related to lockout policies.
	Date/time settings	Settings related to date/time.

	Password quality settings	Settings of the minimum character number and the combination of characters to be registered for user authentication regarding the password policy.
	Auto Logout settings	Auto Logout settings for the Operation Panel and Auto Logout settings for the WIM.
	S/MIME user information	Information required for e-mail transmission of attachments using S/MIME. This information consists of items set for each user (e-mail address and user certificate) and S/MIME setting (encryption setting). This information is registered and managed by the MFP administrator.
	Destination folder	Destination information for the folder transmission function. This includes the path information to the destination server and the folder in the server, and information including identification and authentication information for user access. This information is registered and managed by the MFP administrator.
	Audit log settings	Settings related to the transfer of audit logs.
	Cryptographic communication settings	Settings related to TLS and IPsec communication with clients and servers.
	Login user name	User identifier associated with any of the normal user, MFP administrator, or supervisor. The TOE identifies users by this identifier.
	User role	Any role of normal user, MFP administrator, or supervisor who uses the TOE.
	Document data owner information	The security attribute of the document data. The owner information of the document data (the login user name) is set. For the document data received via a telephone line (+DSR, Fax reception document), the list of login user names is set.
	List for users who have been granted access permission for the document data	The security attribute of the document data (+DSR), excluding the document data received via a telephone line (Fax reception document). The information of the users (the login user names) who are allowed access (viewing) the document data is set. The document data owner can allow other normal users to read the document data.
	User job data owner information	The security attribute of the user job data. The user job data owner information (the login user name) is set.
	Available function list	The attribute given to normal users. The list of functions (MFP applications) that are allowed to be used is given to normal users.
	Function type	MFP application attribute, such as Copy Function, Printer Function, Scanner Function, Fax Function, and Document Server Function.
TSF confidential data (D.CONF)	Login password	A password associated with each login user name.
	Audit log	Audit log data in which occurred events are recorded.

	HDD cryptographic key	Cryptographic key used to encrypt data in the HDD.

3.3 Threats

Defined and described below are the assumed threats related to the use of this TOE and the operational environment. The threats defined in this section are unauthorised persons with knowledge of published information about the TOE operations. Such attackers are capable of Basic level of attack potential.

T.DOC.DIS **Document data disclosure**

Document data managed by the TOE may be disclosed by unauthorised persons.

T.DOC.ALT **Document data alteration**

Document data managed by the TOE may be altered by unauthorised persons.

T.FUNC.ALT **User job data alteration**

User job data managed by the TOE may be altered by unauthorised persons.

T.PROT.ALT **Alteration of TSF protected data**

TSF protected data managed by the TOE may be altered by unauthorised persons.

T.CONF.DIS **Disclosure of TSF confidential data**

TSF confidential data managed by the TOE may be disclosed by unauthorised persons.

T.CONF.ALT **Alteration of TSF confidential data**

TSF confidential data managed by the TOE may be altered by unauthorised persons.

3.4 Organisational Security Policies

The following organisational security policies are taken.

P.USER.AUTHORIZATION **User identification and authentication**

To maintain operational accountability and security, give users the authority to use the TOE only when authorized by the TOE owner.

P.SOFTWARE.VERIFICATION **Software verification**

To detect corruption of the executable code in TSF, implement procedures to self-test the executable code.

P.AUDIT.LOGGING **Management of audit log records**

To maintain operational accountability and security, create and maintain records that provide audit trail of TOE use and security-relevant events, protect them from unauthorised disclosure and alteration, and make them viewable only by authorised persons.

P.INTERFACE.MANAGEMENT **Management of external interfaces**

To prevent unauthorised use of the external interfaces of the TOE, control the operation of those interfaces by the TOE and its IT environment.

P.STORAGE.ENCRYPTION **Encryption of storage devices**

The data recorded in the TOE's HDD shall be encrypted.

3.5 Assumptions

The assumptions related to this TOE operational environment are identified and described.

A.ACCESS.MANAGED **Access management**

The TOE is placed in a restricted or monitored environment that is protected from unauthorised access to the physical components of the TOE and data interfaces.

A.USER.TRAINING **User training**

Users of the TOE are aware of the security policies and procedures of their organisation, are trained to follow those policies and procedures, and gain competence to follow them.

A.ADMIN.TRAINING **Administrator training**

Administrators are aware of the security policies and procedures of their organisation, are trained to follow the guidance and documents of the manufacturer, gain competence to follow them, and are able to configure and operate the TOE properly according to those policies and procedures.

A.ADMIN.TRUST **Trusted administrator**

Administrators do not use their access rights for malicious purposes.

4 Security Objectives

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

4.1 Security Objectives for TOE

This section describes the security objectives for the TOE.

O.DOC.NO_DIS Protection of document data disclosure

The TOE shall protect document data from being disclosed by unauthorised persons.

O.DOC.NO_ALT Protection of document data alteration

The TOE shall protect document data from being altered by unauthorised persons.

O.FUNC.NO_ALT Protection of user job data alteration

The TOE shall protect user job data from being altered by unauthorised persons.

O.PROT.NO_ALT Protection of TSF protected data alteration

The TOE shall protect TSF protected data from being altered by unauthorised persons.

O.CONF.NO_DIS Protection of TSF confidential data disclosure

The TOE shall protect TSF confidential data from being disclosed by unauthorised persons.

O.CONF.NO_ALT Protection of TSF confidential data alteration

The TOE shall protect TSF confidential data from being altered by unauthorised persons.

O.USER.AUTHORIZED User identification and authentication

The TOE shall require identification and authentication of users, give users the access rights according to the security policies, and then ensure that users are allowed to use the TOE.

O.INTERFACE.MANAGED Management of external interfaces by TOE

The TOE shall manage the operation of external interfaces in accordance with the security policies.

O.SOFTWARE.VERIFIED Software verification

The TOE shall provide procedures to self-verify the executable code in the TSF.

O.AUDIT.LOGGED Management of audit log records

The TOE shall record and manage events related to the TOE use and security, and prevent unauthorised disclosure and alteration.

O.STORAGE.ENCRYPTED Encryption of storage devices

The TOE shall ensure that data to be written to the HDD is encrypted first and then recorded.

4.2 Security Objectives for Operational Environment

This section describes the security objectives for the operational environment.

4.2.1 IT Environment

OE.AUDIT_STORAGE.PROTECTED Audit log protection in trusted IT products

When exporting audit records from the TOE to another trusted IT product, the TOE owner shall ensure that the audit records are protected from unauthorized access, deletion, and alteration.

OE.AUDIT_ACCESS.AUTHORIZED Audit log access control in trusted IT products

When exporting audit records generated by the TOE from the TOE to another trusted IT product, the TOE owner shall ensure that those records can be accessed in order to detect potential security violations, and only by authorized persons.

OE.INTERFACE.MANAGED Management of external interfaces in IT environment

The IT environment shall provide protection against the unauthorised access to the TOE external interfaces.

4.2.2 Non-IT Environment

OE.PHYSICAL.MANAGED Physical management

The TOE shall be placed in a secure or monitored area that is protected from unauthorised physical access to the TOE.

OE.USER.AUTHORIZED Assignment of user authority

The TOE owner shall give users the authority to use the TOE according to the organisational security policies and procedures.

OE.USER.TRAINED **User training**

The TOE owner shall ensure that users of the TOE are aware of the security policies and procedures of their organisation, are trained to follow those policies and procedures, and gain competence to follow them.

OE.ADMIN.TRAINED **Administrator training**

The TOE owner shall ensure that administrators are aware of the security policies and procedures of their organisation, are trained to follow the guidance and documents of the manufacturer, secure time to gain competence to follow them, and are able to configure and operate the TOE properly according to those policies and procedures.

OE.ADMIN.TRUSTED **Trusted administrator**

The TOE owner shall establish trust so that administrators will not use their access privilege for malicious purposes.

OE.AUDIT.REVIEWED **Log audit**

The TOE owner shall ensure that audit logs are reviewed at appropriate intervals for detecting security violations or unusual patterns of activity.

4.3 Security Objectives Rationale

This section describes the rationale for security objectives. The security objectives are for upholding the assumptions, countering the threats, and enforcing the organisational security policies, which are defined.

4.3.1 Correspondence Table of Security Objectives

Table 13 describes the correspondence between the security objectives, and the assumptions to be upheld, threats to be countered and organisational security policies to be enforced.

Table 13 : Rationale for 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	OE.USER.AUTHORIZED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED	OE.AUDIT_STORAGE.PROTCTED	OE.AUDIT_ACCESS_AUTHORIZED	OE.AUDIT.REVIEWED	O.INTERFACE.MANAGED	O.STORAGE.ENCRYPTED	OE.INTERFACE.MANAGED	OE.PHYSICAL.MANAGED	OE.ADMIN.TRAINED	OE.ADMIN.TRUSTED	OE.USER.TRAINED
T.DOC.DIS	X						X	X												
T.DOC.ALT		X					X	X												
T.FUNC.ALT			X				X	X												
T.PROT.ALT				X			X	X												
T.CONF.DIS					X		X	X												
T.CONF.ALT						X	X	X												
P.USER.AUTHORIZATION							X	X												
P.SOFTWARE.VERIFICATION									X											
P.AUDIT.LOGGING										X	X	X	X							
P.INTERFACE.MANAGEMENT														X		X				
P.STORAGE.ENCRYPTION															X					
A.ACCESS.MANAGED																	X			
A.ADMIN.TRAINING																		X		
A.ADMIN.TRUST																			X	
A.USER.TRAINING																				X

4.3.2 Security Objectives Descriptions

The following describes the rationale for each security objective being appropriate to satisfy the threats, assumptions, and organisational security policies.

T.DOC.DIS

T.DOC.DIS is countered by O.DOC.NO_DIS, O.USER.AUTHORIZED, and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, the TOE owner gives users the authority to use the TOE according to the organisational security policies and procedures. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, gives users the access rights according to the security policies, and then ensures that users are allowed to use the TOE. By O.DOC.NO_DIS, the TOE protects document data from being disclosed by unauthorised persons.

T.DOC.DIS is countered by these objectives.

T.DOC.ALT

T.DOC.ALT is countered by O.DOC.NO_ALT, O.USER.AUTHORIZED, and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, the TOE owner gives users the authority to use the TOE according to the organisational security policies and procedures. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, gives users the access rights according to the security policies, and then ensures that users are allowed to use the TOE. By O.DOC.NO_ALT, the TOE protects document data from being altered by unauthorised persons.

T.DOC.ALT is countered by these objectives.

T.FUNC.ALT

T.FUNC.ALT is countered by O.FUNC.NO_ALT, O.USER.AUTHORIZED, and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, the TOE owner gives users the authority to use the TOE according to the organisational security policies and procedures. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, gives users the access rights according to the security policies, and then ensures that users are allowed to use the TOE. By O.FUNC.NO_ALT, the TOE protects user job data from being altered by unauthorised persons.

T.FUNC.ALT is countered by these objectives.

T.PROT.ALT

T.PROT.ALT is countered by O.PROT.NO_ALT, O.USER.AUTHORIZED, and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, the TOE owner gives users the authority to use the TOE according to the organisational security policies and procedures. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, gives users the access rights according to the security policies, and then ensures that users are allowed to use the TOE. By O.PROT.NO_ALT, the TOE protects TSF protected data from being altered by unauthorised persons.

T.PROT.ALT is countered by these objectives.

T.CONF.DIS

T.CONF.DIS is countered by O.CONF.NO_DIS, O.USER.AUTHORIZED, and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, the TOE owner gives users the authority to use the TOE according to the organisational security policies and procedures. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, gives users the access rights according to the security policies, and then ensures that users are allowed to use the TOE. By O.CONF.NO_DIS, the TOE protects TSF confidential data from being disclosed by unauthorised persons.

T.CONF.DIS is countered by these objectives.

T.CONF.ALT

T.CONF.ALT is countered by O.CONF.NO_ALT, O.USER.AUTHORIZED, and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, the TOE owner gives users the authority to use the TOE according to the organisational security policies and procedures. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, gives users the access rights according to the security policies, and then ensures that users are allowed to use the TOE. By O.CONF.NO_ALT, the TOE protects TSF confidential data from being altered by unauthorised persons.

T.CONF.ALT is countered by these objectives.

P.USER.AUTHORIZATION

P.USER.AUTHORIZATION is enforced by O.USER.AUTHORIZED and OE.USER.AUTHORIZED.

By OE.USER.AUTHORIZED, the TOE owner gives users the authority to use the TOE according to the organisational security policies and procedures. By O.USER.AUTHORIZED, the TOE requires identification and authentication of users, gives users the access rights according to the security policies, and then ensures that users are allowed to use the TOE.

P.USER.AUTHORIZATION is enforced by these objectives.

P.SOFTWARE.VERIFICATION

P.SOFTWARE.VERIFICATION is enforced by O.SOFTWARE.VERIFIED.

By O.SOFTWARE.VERIFIED, the TOE provides procedures to self-verify the executable code in the TSF.

P.SOFTWARE.VERIFICATION is enforced by this objective.

P.AUDIT.LOGGING

P.AUDIT.LOGGING is enforced by O.AUDIT.LOGGED, OE.AUDIT.REVIEWED, OE.AUDIT_STORAGE.PROTECTED, and OE.AUDIT_ACCESS.AUTHORIZED.

By O.AUDIT.LOGGED, the TOE records and manages events related to the TOE use and security and prevents unauthorised disclosure or alteration. By OE.AUDIT.REVIEWED, the TOE owner ensures that audit logs are reviewed at appropriate intervals for detecting security violations or unusual patterns of activity.

By OE.AUDIT_STORAGE.PROTECTED, when audit records are exported from the TOE to another trusted IT product, the TOE owner ensures to protect those records from unauthorised access, deletion, and alteration. By OE.AUDIT_ACCESS.AUTHORIZED, when audit records generated by the TOE are exported from the

TOE to another trusted IT product, the TOE owner detects potential security violations and ensures that only authorised persons can access those records.

P.AUDIT.LOGGING is enforced by these objectives.

P.INTERFACE.MANAGEMENT

P.INTERFACE.MANAGEMENT is enforced by O.INTERFACE.MANAGED and OE.INTERFACE.MANAGED.

By O.INTERFACE.MANAGED, the TOE manages the operation of the external interfaces in accordance with the security policies. By OE.INTERFACE.MANAGED, the IT environment provides protection against unauthorised access to the TOE external interfaces.

P.INTERFACE.MANAGEMENT is enforced by these objectives.

P.STORAGE.ENCRYPTION

P.STORAGE.ENCRYPTION is enforced by O.STORAGE.ENCRYPTED.

By O.STORAGE.ENCRYPTED, the TOE ensures that data to be written to the HDD is encrypted and the encrypted data is recorded in the HDD.

P.STORAGE.ENCRYPTION is enforced by this objective.

A.ACCESS.MANAGED

A.ACCESS.MANAGED is upheld by OE.PHYSICAL.MANAGED.

By OE.PHYSICAL.MANAGED, the TOE is placed in a secure or monitored area that is protected from unauthorised physical access to the TOE.

A.ACCESS.MANAGED is upheld by this objective.

A.ADMIN.TRAINING

A.ADMIN.TRAINING is upheld by OE.ADMIN.TRAINED.

By OE.ADMIN.TRAINED, the TOE owner ensures that administrators are aware of the security policies and procedures of their organisation, are trained to follow the guidance and documents of the manufacturer, secure time to gain competence to follow them, and are able to configure and operate the TOE properly according to those policies and procedures.

A.ADMIN.TRAINING is upheld by this objective.

A.ADMIN.TRUST

A.ADMIN.TRUST is upheld by OE.ADMIN.TRUSTED.

By OE.ADMIN.TRUSTED, the TOE owner establishes trust so that administrators will not use their access privilege for malicious purposes.

A.ADMIN.TRUST is upheld by this objective.

A.USER.TRAINING

A.USER.TRAINING is upheld by OE.USER.TRAINED.

By OE.USER.TRAINED, the TOE owner ensures that users of the TOE are aware of the security policies and procedures of their organisation, are trained to follow those policies and procedures, and gain competence to follow them.

A.USER.TRAINING is upheld by this objective.

5 Extended Components Definition

This section describes Extended Components Definition.

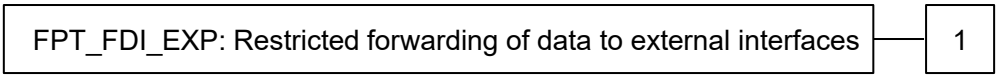
5.1 Restricted forwarding of data to external interfaces (FPT_FDI_EXP)

Family behaviour

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

Many products are intended to receive information on specific external interfaces, and 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 levelling:



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 ST, the authors needed to express the control of both user data and TSF data flow using administrative control instead of attribute-based control. It is considered inappropriate to use FDP_IFF and FDP_IFC by applying refinement for this purpose. 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.

The terms used in this section are defined below.

Table 14 : Terms Used in Section 6

Classification of Term	Name of Term	Description of Term
Subject	Normal user process	A process that acts on behalf of a normal user when the authentication of the normal user is successful.
	MFP administrator process	A process that acts on behalf of an MFP administrator when the authentication of the MFP administrator is successful.
	Supervisor process	A process that acts on behalf of a supervisor when the authentication of the supervisor is successful.
Object	Document data (D.DOC)	Paper documents, digitised documents, deleted documents, temporary documents, or their fragments managed by the TOE.
	User job data (D.FUNC)	Information related to the user's document or document processing job.
	MFP application	General term for Copy Function, Printer Function, Scanner Function, Fax Function, and Document Server Function enforcing SFR package functions in PP (F.CPY, F.PRT, F.SCN, F.FAX, and F.DSR).
	F.CPY	Copying: a function in which physical document input is duplicated to physical document output
	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.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

Classification of Term	Name of Term	Description of Term
	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
Operation	Read	To perform print, download, fax transmission, e-mail transmission of attachments, folder transmission, preview, or fax reception.
	Delete	To delete TSF data or objects.
	Modify	To modify TSF data or objects.
	Query	To refer to TSF data.
	Newly create	To newly create TSF data.
	Change_default	To change the default value of TSF data.
	Execute	To execute MFP application jobs.
Security attribute	Login user name	User identifier associated with any of the normal user, MFP administrator, or supervisor. The TOE identifies users by this identifier.
	User role	Any role of normal user, MFP administrator, or supervisor who uses the TOE.
	Document data attribute	The security attribute that identifies SFR package functions in PP. This is associated with the document data (D.DOC) and the user job data (D.FUNC). This attribute includes +PRT, +SCN, +CPY, +FAXOUT, +FAXIN, and +DSR. This is a security attribute that is not used in the TOE implementation.
	+PRT	One of the document data attributes. It refers to data associated with a print job.
	+SCN	One of the document data attributes. It refers to data associated with a scan job.
	+CPY	One of the document data attributes. It refers to data associated with a copy job.
	+FAXOUT	One of the document data attributes. It refers to data associated with an outbound (transmission) fax job.

Classification of Term	Name of Term	Description of Term
	+FAXIN	One of the document data attributes. It refers to data associated with an inbound (reception) fax job.
	+DSR	One of the document data attributes. It refers to data associated with a job for saving and retrieving documents.
	Document data owner information	The security attribute of the document data. The document data owner information (the login user name) is set. For the document data received via a telephone line (+DSR, Fax reception document), the list of login user names is set.
	List for users who have been granted access permission for the document data	The security attribute of the document data (+DSR), excluding the document data received via a telephone line (Fax reception document). The information of the users (the login user names) who are allowed access (viewing) the document data is set. The document data owner can allow other normal users to read the document data.
	User job data owner information	The security attribute of the user job data. The user job data owner information (the login user name) is set.
	Available function list	The attribute given to normal users. The list of functions (MFP applications) that are allowed to be used is given to normal users.
	Function type	MFP application attribute, such as Copy Function, Printer Function, Scanner Function, Fax Function, and Document Server Function.
External entity	Normal user	A user who is allowed to use the TOE. A normal user is provided with a login user name, and can use the MFP applications.

Classification of Term	Name of Term	Description of Term
	MFP administrator	A user who has the privilege to manage the TOE, including: - Operation of configuration of normal user settings - Operation of setting information related to MFP device behaviour - Operation of audit logs - Operation of configuration of network settings - Access management of fax reception document - Unlocking locked-out normal users and a supervisor
	Supervisor	A user who has the privilege to manage the TOE, including: - Changing login password of MFP administrators - Unlocking locked-out MFP administrators
Other terms	MFP Control Software	A software component installed in the TOE. This component is stored in FlashROM.
	Operation Panel Control Software	A software component installed in the TOE. This component is stored in the Operation Panel Control Board of the Operation Panel.

6.1 Security Functional Requirements

This section describes the TOE security functional requirements for fulfilling the security objectives defined in section 4.1. The security functional requirements are quoted from the requirement defined in the CC Part 2. The security functional requirements that are not defined in CC Part 2 are quoted as defined in the SMI SFR Package for extended security functional requirements defined in the PP.

The part with assignment and selection defined in the [CC] is identified with **[bold face and brackets]**.

6.1.1 Class FAU: Security audit

6.1.1.1. 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:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the **[selection: not specified]** level of audit; and
c) **[assignment: auditable events of the TOE shown in Table 15]**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome

(success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: types of job for FDP_ACF.1(a), all login user names that attempted the user identification for FIA_UID.1, communicating devices with the trusted channel, lockout operation type, locked out user, and locked out user who is to be released]**.

Table 15 : List of Auditable Events

Auditable Event	Related SFR
Download and deletion of audit logs	FAU_STG.1 FAU_SAR.1 FAU_SAR.2
- Start and end of creating document data - Start and end of printing document data - Start and end of downloading document data - Start and end of sending document data by fax transmission - Start and end of sending document data by e-mail transmission of attachments - Start and end of sending document data by folder transmission - Start and end of deletion of document data - Deletion of user job data Those described above, "creating, printing, and downloading document data, sending document data by fax transmission, e-mail transmission of attachments, and folder transmission, deletion of document data, and deletion of user job data", correspond to the job types.	FDP_ACF.1(a)
Starting and releasing lockout	FIA_AFL.1
Success and failure of login operations	FIA_UAU.1
Success and failure of login operations. Also includes the user identification that is required by the PP as the additional information.	FIA_UID.1
Use of the management functions in Table 31	FMT_SMF.1 FPT_STM.1
Termination of session by Auto Logout	FTA_SSL.3
Failure of the trusted channel functions	FTP_ITC.1
No record because there is no function for modifications to the group of users	FMT_SMR.1

6.1.1.2. 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.

6.1.1.3. FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

6.1.1.4. FAU_STG.4 Prevention of audit data loss

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

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall **[selection: overwrite the oldest stored audit records]** and **[assignment: no other actions to be taken in case of audit storage failure]** if the audit trail is full.

6.1.1.5. 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: the MFP administrators]** with the capability to read **[assignment: all of log items]** from the audit records.

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

6.1.1.6. FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

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

6.1.2 Class FCS: Cryptographic support

6.1.2.1. FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: random number generation using AES-128]** and specified cryptographic key sizes **[assignment: 256 bits]** that meet the following: **[assignment: none]**.

6.1.2.2. FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

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

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: overwriting with 0]** that meets the following: **[assignment: none]**.

6.1.2.3. FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

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

FCS_COP.1.1 The TSF shall perform **[assignment: encryption of data to be written to the HDD, Decryption of data to be read from the HDD]** in accordance with a specified cryptographic algorithm **[assignment: AES]** and cryptographic key sizes **[assignment: 256 bits]** that meet the following: **[assignment: FIPS197]**.

6.1.3 Class FDP: User data protection

6.1.3.1. FDP_ACC.1(a) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(a) The TSF shall enforce the **[assignment: user data access control SFP]** on **[assignment: list of subjects, objects, and operations among subjects and objects in Table 16]**.

Table 16 : List of Subjects, Objects, and Operations among Subjects and Objects (a)

Subjects	Object	Operations
Normal user process MFP administrator process Supervisor process	Document data (D.DOC)	Read Delete
	User job data (D.FUNC)	Modify Delete

6.1.3.2. FDP_ACC.1(b) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(b) The TSF shall enforce the **[assignment: TOE function access control SFP]** on **[assignment: list of subjects, objects, and operations among subjects and objects in Table 17]**.

Table 17 : List of Subjects, Objects, and Operations among Subjects and Objects (b)

Subject	- Normal user process - MFP administrator process - Supervisor process
Object	- MFP application
Operation	- Execute

6.1.3.3. 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 **[assignment: user data access control SFP]** to objects based on the followings: **[assignment: subjects or objects, and their corresponding security attributes shown in Table 18]**.

Table 18 : Subjects, Objects and Security Attributes (a)

Category	Subject or Object	Security Attribute
Subject	Normal user process	- Login user name - User role
Subject	MFP administrator process	- Login user name - User role
Subject	Supervisor process	- Login user name - User role
Object	Document data (D.DOC)	- Document data attribute - Document data owner information - List for users who have been granted access permission for the document data
Object	User job data (D.FUNC)	- Document data attribute - User job data owner information

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: **[assignment: rules to control operations among objects and subjects shown in Table 19]**.

Table 19 : Rules to Control Operations on Document Data and User Job Data (a)

Object	Document Data Attribute	Operation	Subject	Rule to Control Operations
Document data (D.DOC)	+PRT +SCN +FAXOUT +CPY	Delete	Normal user process	Denied, except for his/her own documents.
Document data (D.DOC)	+PRT	Read	Normal user process	Denied, except for his/her own documents.
Document data (D.DOC)	+SCN +FAXOUT +CPY	Read	Normal user process	Denied, except for his/her own documents. (*1)
Document data (D.DOC)	+FAXIN	Delete Read	Normal user process	Not allowed. (*1)
Document data (D.DOC)	+DSR	Delete	Normal user process	Denied, except for his/her own documents.
Document data (D.DOC)	+DSR	Read	Normal user process	Denied, except for his/her own documents. If the document data owner allows another user to read the document data, the authorized user can read the document data.
User job data (D.FUNC)	+PRT +SCN +FAXOUT +CPY +DSR	Delete	Normal user process	Denied, except for his/her own user job data.
User job data (D.FUNC)	+FAXIN	Delete	Normal user process	Not allowed. (*1)
User job data (D.FUNC)	+PRT +SCN +FAXOUT +FAXIN +CPY +DSR	Modify	Normal user process	Not allowed. (*1)

(*1) No interface is provided.

FDP_ACF.1.3(a) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules to authorise operations among objects and subjects shown in Table 20]**.

Table 20 : Rules to Authorise Operations on Document Data and User Job Data (a)

Object	Document Data Attribute	Operation	Subject	Rule to Authorise Operations
Document data (D.DOC)	+PRT +SCN +FAXOUT +CPY	Delete	MFP administrator process	Allowed.
Document data (D.DOC)	+DSR	Delete Read	MFP administrator process	Allowed.
Document data (D.DOC)	+FAXIN	Read	MFP administrator process	Allowed.
User job data (D.FUNC)	+PRT +SCN +FAXOUT +CPY +DSR	Delete	MFP administrator process	Allowed.

FDP_ACF.1.4(a) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: rules to deny operations among objects and subjects shown in Table 21]**.

Table 21 : Rules to Deny Operations on Document Data and User Job Data (a)

Object	Document Data Attribute	Operation	Subject	Rule to Deny Operations
Document data (D.DOC)	+FAXIN	Delete	MFP administrator process	Not allowed. (*1)
Document data (D.DOC)	+PRT +SCN +FAXOUT +CPY	Read	MFP administrator process	Not allowed. (*1)
Document data (D.DOC)	+PRT +SCN +FAXOUT +FAXIN +CPY +DSR	Delete Read	Supervisor process	Not allowed. (*1)
User job data (D.FUNC)	+FAXIN	Delete	MFP administrator process	Not allowed. (*1)

Object	Document Data Attribute	Operation	Subject	Rule to Deny Operations
User job data (D.FUNC)	+PRT +SCN +FAXOUT +FAXIN +CPY +DSR	Modify	MFP administrator process	Not allowed. (*1)
User job data (D.FUNC)	+PRT +SCN +FAXOUT +FAXIN +CPY +DSR	Delete Modify	Supervisor process	Not allowed. (*1)

(*1) No interface is provided.

6.1.3.4. 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 **[assignment: TOE function access control SFP]** to objects based on the following: **[assignment: subjects or objects, and their corresponding security attributes shown in Table 22]**.

Table 22 : Subjects, Objects and Security Attributes (b)

Category	Subject or Object	Security Attribute
Subject	Normal user process	Login user name Available function list User role
Subject	MFP administrator process	Login user name User role
Subject	Supervisor process	Login user name User role
Object	MFP application	Function type

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: **[assignment: rules to control operations among objects and subjects shown in Table 23]**.

Table 23 : Rule to Control Operations on MFP Applications (b)

Object	Operation	Subject	Rule to Control Operations
MFP applications (F.CPY, F.PRT, F.SCN, F.FAX, F.DSR)	Execute	Normal user process	Allows the execution of MFP applications whose function type matches those allowed in the available function list for normal user process.

FDP_ACF.1.3(b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: authorise the execution of the MFP application if the user role of the MFP administrator process is MFP administrator]**.

FDP_ACF.1.4(b) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: deny the execution of the MFP application if the user role of the supervisor process is supervisor]**.

6.1.3.5. 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: deallocation of the resource from]** the following objects: **[assignment: document data]**.

6.1.4 Class FIA: Identification and authentication

6.1.4.1. 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: an administrator configurable positive integer within [assignment: 1 to 5]]** unsuccessful authentication attempts occur related to **[assignment: the authentication events shown in Table 24]**.

Table 24 : List of Authentication Events

Authentication Event
User authentication using the Operation Panel
User authentication using the WIM
User authentication when document data is received from the printer driver and temporarily saved or stored
User authentication when document data is received from the fax driver and stored

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **[selection: met, surpassed]**, the TSF shall **[assignment: perform actions shown in Table 25]**.

Table 25 : List of Actions for Authentication Failure

Unsuccessfully Authenticated User	Action for Authentication Failure
Normal user	The normal user is locked out during the lockout time set by the MFP administrator, or until the MFP administrator performs the release operation.
MFP administrator	The MFP administrator is locked out during the lockout time set by the MFP administrator, until the supervisor performs the release operation, or until a given time elapses after the TOE restarts.
Supervisor	The supervisor is locked out during the lockout time set by the MFP administrator, until the MFP administrator performs the release operation, or until a given time elapses after the TOE restarts.

6.1.4.2. 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: login user name, available function list, and user role]**

6.1.4.3. 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 meet **[assignment: the following quality metrics]**.

(1) To use multiple character types of upper-case letters, lower-case letters, digits, and symbols. (The required number of types is set by the MFP administrator as the password complexity setting.)

(2) Passwords must be single-byte alphanumeric letters and symbols with minimum character number of password (8 to 32 characters set by the MFP administrator) or more, and

- Must be 128 characters or less for normal users
- Must be 32 characters or less for MFP administrators and a supervisor

6.1.4.4. 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: the viewing of the list of user job data, the viewing of WIM Help, the viewing of system status, the viewing of counter, the viewing of information of**

inquiries, and execution of fax reception] on behalf of the user to be performed before the user is authenticated.

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.

6.1.4.5. 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: dummy letters displayed as authentication feedback]** to the user while the authentication is in progress.

6.1.4.6. FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow **[assignment: the viewing of the list of user job data, the viewing of WIM Help, the viewing of system status, the viewing of counter, the viewing of information of inquiries, and execution of fax reception]** on behalf of the user to be performed before the user is identified.

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

6.1.4.7. 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: login user name, available function list, and user role]**

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[assignment: no rules for the initial association of attributes]**

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

6.1.5 Class FMT: Security management

6.1.5.1. FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [**selection: disable, enable**] the function [**assignment: syslog transfer function**] to [**assignment: the MFP administrator**].

6.1.5.2. 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 **[assignment: user data access control SFP]** to restrict the ability to **[selection: delete, change_default, [assignment: newly create, modify]]** the security attributes **[assignment: security attributes in Table 26]** to **[assignment: the user roles with operation permission in Table 26]**.

Table 26 : User Roles for Security Attributes (a)

Security Attribute	Operation	User Role with Operation Permission
Login user name [When associated with a normal user]	Newly create Modify Delete	MFP administrator
Login user name [When associated with an MFP administrator]	Newly create	MFP administrator
	Modify	MFP administrator in question
Login user name [When associated with a supervisor]	Modify	Supervisor
User role	Modify	No role with the operation permission
Document data owner information [+PRT, +SCN, +FAXOUT, +FAXIN, +CPY]	Modify	No role with the operation permission
Document data owner information [+DSR: Other than the document data received via a telephone line]	Modify	No role with the operation permission
Document data owner information [+DSR: Document data received via a telephone line]	Modify	MFP administrator
List for users who have been granted access permission for the document data	Modify	MFP administrator Document data owner (Normal user)
	Change_default	MFP administrator
User job data owner information	Modify	No role with the operation permission

6.1.5.3. FMT_MSA.1(b) Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1(b) The TSF shall enforce the TOE function access control SFP **[assignment: TOE function access control SFP]** to restrict the ability to **[selection: delete, [assignment: newly create, modify]]** the security attributes **[assignment: security attributes in Table 27]** to **[assignment: the user roles with operation permission in Table 27]**.

Table 27 : User Roles for Security Attributes (b)

Security Attribute	Operation	User Role with Operation Permission
Login user name [When associated with a normal user]	Newly create Modify Delete	MFP administrator
Login user name [When associated with an MFP administrator]	Newly create	MFP administrator
	Modify	MFP administrator in question
Login user name [When associated with a supervisor]	Modify	Supervisor
User role	Modify	No role with the operation permission
Available function list	Newly create Modify Delete	MFP administrator
Function type	Modify	No role with the operation permission

6.1.5.4. 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 **[assignment: user data access control SFP]** to provide **[selection: restrictive]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(a) The TSF shall allow the **[assignment: authorised identified roles shown in Table 28]** to specify alternative initial values to overwrite the default values when an object or information is created.

Table 28 : Authorised Identified Roles Allowed to Overwrite Default Values

Object	Security Attribute	Authorised Identified Role
Document data (D.DOC)	Document data owner information	No authorised identified roles
Document data (D.DOC)	List for users who have been granted access permission for the document data	Normal user who creates the document data (Allowed only when storing document data from the Operation Panel. There is no interface for overwriting default values when storing document data from the printer driver.)
User job data (D.FUNC)	User job data owner information	No authorised identified roles

6.1.5.5. 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 **[assignment: TOE function access control SFP]** to provide **[selection: restrictive]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(b) The TSF shall allow the **[assignment: no authorised identified roles]** to specify alternative initial values to overwrite the default values when an object or information is created.

6.1.5.6. FMT_MTD.1(a) 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: query, delete, [assignment: newly create, modify]]** the **[assignment: list of TSF data in Table 29]** to **[assignment: the user roles in Table 29]**.

Table 29 : List of TSF Data

Category	TSF Data	Operation	User Role
TSF protected data (D.PROT)	Lockout settings	Modify	MFP administrator
	Date/time settings	Modify	MFP administrator
	Password quality settings	Modify	MFP administrator
	Auto Logout settings	Modify	MFP administrator
	S/MIME user information	Newly create Modify Delete	MFP administrator

Category	TSF Data	Operation	User Role
	Destination folder	Newly create Modify Delete	MFP administrator
	Audit log settings	Modify	MFP administrator
	Cryptographic communication settings	Modify	MFP administrator
TSF confidential data (D.CONF)	Login password [When associated with a normal user]	Newly create	MFP administrator
		Modify	Normal user in question MFP administrator
	Login password [When associated with an MFP administrator]	Newly create	MFP administrator
		Modify	MFP administrator in question Supervisor
	Login password [When associated with a supervisor]	Modify	Supervisor
	HDD cryptographic key	Query Delete Newly create	MFP administrator

6.1.5.7. FMT_MTD.1(b) 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(b) The TSF shall restrict the ability to **[selection: query]** the **[assignment: list of TSF data in Table 30]** to **[assignment: the user roles in Table 30]**.

Table 30 : List of TSF Data

Category	TSF Data	Operation	User Role
TSF confidential data (D.CONF)	Login password	Query	No role with the operation permission

6.1.5.8. 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: management functions shown in Table 31]**

Table 31 : List of Specification of Management Functions

Management Function
Disable and enable the syslog transfer function
Modify lockout settings
Modify date/time settings
Modify password quality settings
Modify Auto Logout settings
Newly create, modify, and delete S/MIME user information
Newly create, modify, and delete destination folders
Modify audit log settings
Modify cryptographic communication settings
Newly create and modify login passwords
Newly create, modify, and delete login user names
Modify document data (+DSR: Document data received via a telephone line) owner information
Modify the list for users who have been granted access permission for the document data, and change the default value of it
Newly create, modify, and delete the available function list
Query, delete, and newly create HDD cryptographic keys

6.1.5.9. 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 **[assignment: normal user, MFP administrator, and supervisor]**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6 Class FPT: Protection of the TSF

6.1.6.1. 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.

6.1.6.2. 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]** to demonstrate the correct operation of **[selection: [assignment: the MFP Control Software, Operation Panel Control Software]]**.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **[selection: [assignment: HDD cryptographic key]]**.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of **[selection: [assignment: the stored TSF executable code]]**.

6.1.6.3. FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

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

6.1.7 Class FTA: TOE access

6.1.7.1. FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate the interactive session after **[assignment: the time specified by the MFP administrator]**.

6.1.8 Class FTP: Trusted path/channels

6.1.8.1. 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 **[selection: 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 **[assignment: communication via the LAN of document data, user job data, TSF protected data, and TSF confidential data]**.

6.2 Security Assurance Requirements

The evaluation assurance level of this TOE is EAL2+ALC_FLR.2. Table 32 lists the assurance components of the TOE. ALC_FLR.2 was added to the set of components defined in evaluation assurance level 2 (EAL2).

Table 32 : TOE Security Assurance Requirements (EAL2+ALC_FLR.2)

Assurance Class	Assurance Component	
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
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 for security requirements.

If all security functional requirements are satisfied as below, the security objectives for TOE defined in "4 Security Objectives" are fulfilled.

6.3.1 Tracing

Table 33 describes the relationship between the security functional requirements and security objectives for TOE. Items in **bold** provide the primal (**P**) fulfillment of the objectives, and items in standard typeface support (S) its fulfillment. Table 33 describes that each TOE security functional requirement fulfils at least one TOE security objective.

Table 33 : Correspondence of Security Objectives and Functional 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.STORAGE.ENCRYPTED
FAU_GEN.1										**P**	
FAU_GEN.2										**P**	
FAU_STG.1						**P**				**P**	
FAU_STG.4										S	
FAU_SAR.1					**P**					**P**	
FAU_SAR.2					**P**					**P**	
FCS_CKM.1											S
FCS_CKM.4											S
FCS_COP.1											**P**
FDP_ACC.1(a)	**P**	**P**	**P**								
FDP_ACC.1(b)							**P**				
FDP_ACF.1(a)	**P**	**P**	**P**								
FDP_ACF.1(b)							**P**				
FDP_RIP.1	**P**										
FIA_AFL.1							S				
FIA_ATD.1							S				
FIA_SOS.1							S				
FIA_UAU.1							**P**	**P**			
FIA_UAU.7							S				
FIA_UID.1	S	S	S	S	S	S	**P**	**P**		S	
FIA_USB.1							**P**				

	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.STORAGE.ENCRYPTED
FPT_FDI_EXP.1								**P**			
FMT_MOF.1				**P**							
FMT_MSA.1(a)	S	S	S	**P**							
FMT_MSA.1(b)				**P**			S				
FMT_MSA.3(a)	S	S	S								
FMT_MSA.3(b)							S				
FMT_MTD.1(a)				**P**	**P**	**P**					
FMT_MTD.1(b)					**P**						
FMT_SMF.1	S	S	S	S	S	S					
FMT_SMR.1	S	S	S	S	S	S					
FPT_STM.1										S	
FPT_TST.1									**P**		
FTA_SSL.3							**P**	**P**			
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**					

6.3.2 Justification of Traceability

This section describes below how the TOE security objectives are fulfilled by the TOE security functional requirements corresponding to the TOE security objectives. SFR items in **bold** provide the primal (**P**) fulfillment of the objectives, and SFR items in standard typeface support (S) its fulfillment.

O.DOC.NO_DIS Protection of document disclosure

O.DOC.NO_DIS is a security objective by which the TOE protects document data from being disclosed by unauthorised persons. To fulfil this security objective, it is required to implement the following SFRs.

(1) FDP_ACC.1(a)

FDP_ACC.1(a) defines the access control policy for document data.

(2) FDP_ACF.1(a)

FDP_ACF.1(a) provides the access control functions in accordance with the access control policy for document data.

(3) FDP_RIP.1

FDP_RIP.1 prevents deleted documents, temporary documents and their fragments from being read.

(4) FTP_ITC.1

FTP_ITC.1 protects the document data sent and received by the TOE via the LAN.

(5) FMT_MSA.1(a)

FMT_MSA.1(a) restricts the management of security attributes to specific users.

(6) FMT_MSA.3(a)

FMT_MSA.3(a) manages the default security attributes when the document data is generated.

(7) FIA_UID.1

FIA_UID.1 identifies persons who attempt to use the TOE.

(8) FMT_SMR.1

FMT_SMR.1 maintains the authorised user roles.

(9) FMT_SMF.1

FMT_SMF.1 performs the required management functions for the security functions.

O.DOC.NO_DIS can be fulfilled by satisfying these security functional requirements.

O.DOC.NO_ALT Protection of document alteration

O.DOC.NO_ALT is a security objective by which the TOE protects document data from being altered by unauthorised persons. To fulfil this security objective, it is required to implement the following SFRs.

(1) FDP_ACC.1(a)

FDP_ACC.1(a) defines the access control policy for document data.

(2) FDP_ACF.1(a)

FDP_ACF.1(a) provides the access control functions in accordance with the access control policy for document data.

(3) FTP_ITC.1

FTP_ITC.1 protects the document data sent and received by the TOE via the LAN.

(4) FMT_MSA.1(a)

FMT_MSA.1(a) restricts the management of security attributes to specific users.

(5) FMT_MSA.3(a)

FMT_MSA.3(a) manages the default security attributes when the document data is generated.

(6) FIA_UID.1

FIA_UID.1 identifies persons who attempt to use the TOE.

(7) FMT_SMR.1

FMT_SMR.1 maintains the authorised user roles.

(8) FMT_SMF.1

FMT_SMF.1 performs the required management functions for the security functions.

O.DOC.NO_ALT can be fulfilled by satisfying these security functional requirements.

O.FUNC.NO_ALT Protection of user job data alteration

O.FUNC.NO_ALT is a security objective by which the TOE protects user job data from being altered by unauthorised persons. To fulfil this security objective, it is required to implement the following SFRs.

(1) FDP_ACC.1(a)

FDP_ACC.1(a) defines the access control policy for user job data.

(2) FDP_ACF.1(a)

FDP_ACF.1(a) provides the access control functions in accordance with the access control policy for user job data.

(3) FTP_ITC.1

FTP_ITC.1 protects the user job data sent and received by the TOE via the LAN.

(4) FMT_MSA.1(a)

FMT_MSA.1(a) restricts the management of security attributes to specific users.

(5) FMT_MSA.3(a)

FMT_MSA.3(a) manages the default security attributes when the user job is generated.

(6) FIA_UID.1

FIA_UID.1 identifies persons who attempt to use the TOE.

(7) FMT_SMR.1

FMT_SMR.1 maintains the authorised user roles.

(8) FMT_SMF.1

FMT_SMF.1 performs the required management functions for the security functions.

O.FUNC.NO_ALT can be fulfilled by satisfying these security functional requirements.

O.PROT.NO_ALT Protection of TSF protected data alteration

O.PROT.NO_ALT is a security objective by which the TOE protects TSF protected data from being altered by unauthorised persons. To fulfil this security objective, it is required to implement the following SFRs.

(1) FMT_MOF.1

FMT_MOF.1 allows only MFP administrators to manage the behaviour of the security functions.

(2) FMT_MSA.1(a) and FMT_MSA.1(b)

FMT_MSA.1(a) and FMT_MSA.1(b) restrict the management of security attributes to specific users.

(3) FMT_MTD.1(a)

FMT_MTD.1(a) restricts the operation of TSF protected data to authorised users.

(4) FMT_SMF.1

FMT_SMF.1 performs the required management functions for the security functions.

(5) FMT_SMR.1

FMT_SMR.1 maintains the authorised user roles.

(6) FTP_ITC.1

FTP_ITC.1 protects the TSF protected data sent and received by the TOE via the LAN.

(7) FIA_UID.1
FIA_UID.1 identifies persons who attempt to use the TOE.

O.PROT.NO_ALT can be fulfilled by satisfying these security functional requirements.

O.CONF.NO_DIS Protection of TSF confidential data disclosure

O.CONF.NO_DIS is a security objective by which the TOE protects TSF confidential data from being disclosed by unauthorised persons. To fulfil this security objective, it is required to implement the following SFRs.

(1) FMT_MTD.1(a) and FMT_MTD.1(b)
FMT_MTD.1(a) and FMT_MTD.1(b) restrict the operation of TSF confidential data to authorised users.

(2) FMT_SMF.1
FMT_SMF.1 performs the required management functions for the security functions.

(3) FMT_SMR.1
FMT_SMR.1 maintains the authorised user roles.

(4) FTP_ITC.1
FTP_ITC.1 protects the TSF confidential data sent and received by the TOE via the LAN.

(5) FAU_SAR.1
FAU_SAR.1 allows the MFP administrator to read audit logs in a format that can be audited.

(6) FAU_SAR.2
FAU_SAR.2 prohibits persons other than the MFP administrator from reading the audit logs.

(7) FIA_UID.1
FIA_UID.1 identifies persons who attempt to use the TOE.

O.CONF.NO_DIS can be fulfilled by satisfying these security functional requirements.

O.CONF.NO_ALT Protection of TSF confidential data alteration

O.CONF.NO_ALT is a security objective by which the TOE protects TSF confidential data from being altered by unauthorised persons. To fulfil this security objective, it is required to implement the following SFRs.

(1) FMT_MTD.1(a)
FMT_MTD.1(a) restricts the operation of TSF confidential data to authorised users.

(2) FMT_SMF.1
FMT_SMF.1 performs the required management functions for the security functions.

(3) FMT_SMR.1
FMT_SMR.1 maintains the authorised user roles.

(4) FTP_ITC.1
FTP_ITC.1 protects the TSF confidential data sent and received by the TOE via the LAN.

(5) FAU_STG.1
FAU_STG.1 protects audit logs from alteration.

(6) FIA_UID.1
FIA_UID.1 identifies persons who attempt to use the TOE.

O.CONF.NO_ALT can be fulfilled by satisfying these security functional requirements.

O.USER.AUTHORIZED User identification and authentication

O.USER.AUTHORIZED is a security objective by which the TOE requires user identification and authentication of users, gives users the access rights according to the security policies, and then ensures that users are allowed to use the TOE. To fulfil this security objective, it is required to implement the following SFRs.

(1) FIA_UID.1 and FIA_UAU.1

FIA_UID.1 and FIA_UAU.1 identify and authenticate persons who attempt to use the TOE.

(2) FIA_USB.1

FIA_USB.1 associates the security attributes with the user who is successfully identified and authenticated.

(3) FIA_ATD.1

FIA_ATD.1 maintains each user's security attributes registered in the TOE before performing identification and authentication.

(4) FDP_ACC.1(b)

FDP_ACC.1(b) defines the access control policy that allows users to execute the MFP applications according to the operation permission and user role of MFP applications granted to the successfully identified and authenticated users.

(5) FDP_ACF.1(b)

FDP_ACF.1(b) provides the access control functions in accordance with the access control policy that allows users to execute the MFP applications according to the operation permission and user role of MFP applications granted to the successfully identified and authenticated users.

(6) FIA_UAU.7

FIA_UAU.7 displays dummy letters as authentication feedback on the Operation Panel and prevents the login password from disclosure.

(7) FIA_SOS.1

FIA_SOS.1 accepts only passwords that satisfy the quality metrics specified by the MFP administrator, and makes it difficult to guess the login password.

(8) FIA_AFL.1

FIA_AFL.1 does not allow the user who have repeatedly failed authentication a certain number of times to access to the TOE for a certain period of time.

(9) FTA_SSL.3

FTA_SSL.3 performs Auto Logout when the time specified by the MFP administrator has elapsed since the last operation of the user, terminates the inactive session, and enforces the authorisation.

(10) FMT_MSA.1(b)

FMT_MSA.1(b) restricts the management of security attributes to specific users.

(11) FMT_MSA.3(b)

FMT_MSA.3(b) sets security attributes to restrictive values.

O.USER.AUTHORIZED can be fulfilled by satisfying these security functional requirements.

O.INTERFACE.MANAGED Management of external interfaces by TOE

O.INTERFACE.MANAGED is a security objective by which the TOE manages the operation of the external interfaces in accordance with the security policies. To fulfil this security objective, it is required to implement the following SFRs.

(1) FIA_UID.1 and FIA_UAU.1
FIA_UID.1 identifies persons who attempt to use the TOE, and FIA_UAU.1 authenticates the identified users.

(2) FTA_SSL.3
FTA_SSL.3 performs Auto Logout when the time specified by the MFP administrator has elapsed since the last operation of the user, terminates the inactive session, and performs management of external interfaces.

(3) FPT_FDI_EXP.1
FPT_FDI_EXP.1 prevents data received from an arbitrary external interface from being forwarded without further processing by the TSF to an arbitrary shared media interface.

O.INTERFACE.MANAGED can be fulfilled by satisfying these security functional requirements.

O.SOFTWARE.VERIFIED Software verification

O.SOFTWARE.VERIFIED is a security objective by which the TOE provides procedures to self-verify the executable code in the TSF. To fulfil this security objective, it is required to implement the following SFRs.

(1) FPT_TST.1
FPT_TST.1 verifies the HDD cryptographic key and executable code in the TSF, and performs self-tests for the MFP Control Software and Operation Panel Control Software at the start-up.

O.SOFTWARE.VERIFIED can be fulfilled by satisfying this security functional requirement.

O.AUDIT.LOGGED Management of audit log records

O.AUDIT.LOGGED is a security objective by which the TOE records and manages events related to the TOE use and security, and prevents unauthorised disclosure and alteration. To fulfil this security objective, it is required to implement the following SFRs.

(1) FAU_GEN.1 and FAU_GEN.2
FAU_GEN.1 and FAU_GEN.2 record the events, which should be auditable, with the identification information of the occurrence factor.

(2) FAU_STG.1
FAU_STG.1 protects audit logs from alteration.

(3) FAU_STG.4

FAU_STG.4 overwrites the audit log with the oldest timestamp when an auditable event occurs while the audit log file is full.

(4) FAU_SAR.1

FAU_SAR.1 allows the MFP administrator to read audit logs in a format that can be audited.

(5) FAU_SAR.2
FAU_SAR.2 prohibits persons other than the MFP administrator from reading the audit logs.

(6) FPT_STM.1
FPT_STM.1 provides reliable time stamps.

(7) FIA_UID.1
FIA_UID.1 identifies persons who attempt to use the TOE.

O.AUDIT.LOGGED can be fulfilled by satisfying these security functional requirements.

O.STORAGE.ENCRYPTED Encryption of storage devices

O.STORAGE.ENCRYPTED is a security objective by which the TOE ensures that data to be written to the HDD is encrypted. To fulfil this security objective, it is required to implement the following SFRs.

(1) FCS_CKM.1
FCS_CKM.1 generates cryptographic keys in accordance with a specified algorithm.

(2) FCS_CKM.4

FCS_CKM.4 deletes the cryptographic keys in accordance with a specified method.

(3) FCS_COP.1
FCS_COP.1 encrypts data to be written to the HDD in accordance with the specified algorithm and key sizes, and decrypts data read from the HDD.

O.STORAGE.ENCRYPTED can be fulfilled by satisfying these security functional requirements.

6.3.3 Dependency Analysis

Table 34 describes the results of dependency analysis in this ST for the TOE security functional requirements.

Table 34 : Results of Dependency Analysis of TOE Security Functional Requirements

TOE Security Functional Requirement	Claimed Dependencies	SFR for the ST	Sufficiency
FAU_GEN.1	FPT_STM.1	FPT_STM.1	OK
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.1	OK
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	OK
FAU_STG.4	FAU_STG.1	FAU_STG.1	OK
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	OK
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	OK
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1 FCS_CKM.4	OK

TOE Security Functional Requirement	Claimed Dependencies	SFR for the ST	Sufficiency
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1	OK
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1	OK
FDP_ACC.1(a)	FDP_ACF.1	FDP_ACF.1(a)	OK
FDP_ACC.1(b)	FDP_ACF.1	FDP_ACF.1(b)	OK
FDP_ACF.1(a)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(a) FMT_MSA.3(a)	OK However, since the document data attributes are not used in the implementation, this security attribute is not required for FMT_MSA.3(a).
FDP_ACF.1(b)	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1(b) FMT_MSA.3(b)	OK
FDP_RIP.1	None	None	OK
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	OK
FIA_ATD.1	None	None	OK
FIA_SOS.1	None	None	OK
FIA_UAU.1	FIA_UID.1	FIA_UID.1	OK
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	OK
FIA_UID.1	None	None	OK
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	OK
FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1	OK
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	OK

TOE Security Functional Requirement	Claimed Dependencies	SFR for the ST	Sufficiency
FMT_MSA.1(a)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(a) FMT_SMR.1 FMT_SMF.1	OK However, since no interface is provided to modify user roles, modify document data owner information (+PRT, +SCN, +FAXOUT, +FAXIN, +CPY), modify document data owner information (+DSR: document data other than that received via a telephone line), or modify user job data owner information, these management functions are not required for FMT_SMF.1.
FMT_MSA.1(b)	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1(b) FMT_SMR.1 FMT_SMF.1	OK However, since no interface is provided to modify user roles or modify function types, these management functions are not required for FMT_SMF.1.
FMT_MSA.3(a)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(a) FMT_SMR.1	OK
FMT_MSA.3(b)	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1(b) FMT_SMR.1	OK
FMT_MTD.1(a)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	OK
FMT_MTD.1(b)	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1	OK However, since no interface is provided to query login passwords, this management functions are not required for FMT_SMF.1.
FMT_SMF.1	None	None	OK
FMT_SMR.1	FIA_UID.1	FIA_UID.1	OK
FPT_STM.1	None	None	OK
FPT_TST.1	None	None	OK
FTA_SSL.3	None	None	OK
FTP_ITC.1	None	None	OK

6.3.4 Security Assurance Requirements Rationale

This TOE is an MFP, which is a commercially available product. The MFP is assumed that it will be used in a general office and this TOE does not assume the attackers with Enhanced-Basic or higher level of attack potential.

The evaluation of the TOE design (ADV_TDS.1) is adequate to show the validity of commercially available products. A high attack potential is required for the attacks that circumvent or alter the TSF, which is not covered in this evaluation. Dealing with attacks performed by an attacker possessing Basic attack potential (AVA_VAN.2) is therefore adequate for general needs.

In order to securely operate the TOE continuously, it is important to appropriately remediate the flaw discovered after the start of the TOE operation according to flaw reporting procedure (ALC_FLR.2).

Based on the terms and costs of the evaluation, the evaluation assurance level of EAL2+ALC_FLR.2 is appropriate for this TOE.

7 TOE Summary Specification

This section describes the TOE summary specification for each security function. The security functions are described for each corresponding security functional requirement.

7.1 Audit Function

The Audit Function is to record a log that associates TOE audit events with user identification information as the audit log. Also, this function provides the recorded audit log in a format that can be audited. The recorded audit log can be downloaded and deleted only by the MFP administrator. This function also includes a function to provide reliable time stamps and a control function used when the audit log is full. The audit log can also be transferred to and saved on the syslog server.

FAU_GEN.1

The TOE records the audit log items, shown in Table 36, on the HDD in the TOE when audit events shown in Table 35 occur.

Audit log items include basic log items and expanded log items. Basic log items are recorded whenever audit logs are recorded, and expanded log items are recorded only when audit events occur and the audit log items shown in Table 36 are recorded. Among the auditable events, the failure of the trusted channel functions refers to the failure of the function that performs communications via trusted channels. This function includes WIM communication, folder transmission, e-mail transmission of attachments, temporary saving and storing document data received from the printer driver, storing document data received from the fax driver, and syslog transfer. Therefore, logs of these communication failures are audit events.

Table 35 : List of Audit Events

Audit Event
Start-up of the Audit Function
Shutdown of the Audit Function
Download and deletion of audit logs
Success and failure of login operations
Starting and releasing lockout
Use of the management functions in Table 31
Termination of session by Auto Logout
Failure of WIM communication
Failure of folder transmission
Failure of e-mail transmission of attachments
Failure of temporary saving and storing document data received from the printer driver
Failure of storing document data received from the fax driver
Failure of syslog transfer

Audit Event
Deletion of user job data
Creating (storing) document data
Reading document data (print, download, fax transmission, e-mail transmission of attachments, and folder transmission)
Deletion of document data

Table 36 : List of Audit Log Items

	Audit Log Item	Setting Values of Audit Log Item	Audit Events to Record Audit Logs
Basic Log Items	Starting date/time of an event	Values of the TOE system clock at an event occurrence	- All auditable events shown in Table 35
	Ending date/time of an event	Values of the TOE system clock at an event termination	
	Event types	Audit event identity	
	Subject identity	Login user name of the user who caused the audit event	
	Outcome	Audit event outcome (*1)	
Expanded Log Items	Job types	Creation, print, download, fax transmission, e-mail transmission of attachments, folder transmission, deletion of document data, and deletion of user job data. (For deletion of user job data, the values are recorded in the cancellation details field.)	- Start and end of creating document data - Start and end of printing document data - Start and end of downloading document data - Start and end of sending document data by fax transmission - Start and end of sending document data by e-mail transmission of attachments - Start and end of sending document data by folder transmission - Deletion of document data - Deletion of user job data Those described above, "creating, printing, and downloading document data, sending document data by fax transmission, e-mail transmission of attachments, and folder transmission, deletion of document data, and deletion of user job data", correspond to the job types.
	Login user name	All login user names that attempted the user identification	- Success and failure of login operations

	Audit Log Item	Setting Values of Audit Log Item	Audit Events to Record Audit Logs
	Communicating devices	Communicating IP address	- Failure of WIM communication - Failure of folder transmission - Failure of temporary saving and storing document data received from the printer driver - Failure of storing document data received from the fax driver - Failure of syslog transfer
		Communicating e-mail address for e-mail transmission of attachments	- Failure of e-mail transmission of attachments
	Lockout operation type	Information to identify starting lockout and releasing lockout	- Starting and releasing lockout
	Locked out user	Login user name of a user who is locked out	- Starting and releasing lockout
	Locked out user who is to be released	Login user name of a user who is released from lockout	- Starting and releasing lockout

(*1): Either "success" or "failure" will be recorded. If an audit event is "deletion of document data", only "success" will be recorded.

For the following audit events, "failure" will be recorded.

- Failure of WIM communication
- Failure of folder transmission
- Failure of temporary saving and storing document data received from the printer driver
- Failure of storing document data received from the fax driver
- Failure of syslog transfer
- Failure of e-mail transmission of attachments

FAU_GEN.2

The TOE records the login user name in the audit log so that it can identify who caused the audit event.

FPT_STM.1

The date (year/month/day) and time (hour/minute/second) recorded in the audit log are derived from the system clock of the TOE.

FAU_SAR.1 and FAU_SAR.2

The TOE provides the MFP administrators with all audit logs in a text format. The TOE allows the MFP administrator to download audit logs with the WIM only when the MFP administrator accesses it. The TOE does not provide an interface for downloading audit logs to all users except the MFP administrators.

FAU_STG.1

The TOE allows only the MFP administrators to delete audit logs. To delete audit logs, the WIM or the Operation Panel will be used. The TOE does not provide an interface for making partial changes to audit logs.

FAU_STG.4

The TOE writes the newest audit log over the oldest audit log when there is insufficient space in the audit log files to append the newest audit log.

7.2 Identification and Authentication Function

The Identification and Authentication Function is to verify whether a person who attempts to use the TOE is an authorised user based on the login user name and login password entered by the user, so that the TOE can allow only the authenticated users to use the TOE and reject the users when the authentication fails. The lockout function, password protection function, and Auto Logout function are also included in this function.

FIA_UAU.1 and FIA_UID.1

The TOE identifies and authenticates a user with the login user name and login password.

Before the Operation Panel or the WIM is used, the TOE displays the login screen and prompts the user to enter the login user name and login password.
In addition, when the TOE receives a request from the printer driver or fax driver, the TOE receives the login user name and login password entered by a user at the same time as the request.
The TOE performs identification and authentication by checking whether the login user name and login password entered by the user match the login user name and login password registered in the TOE in advance. If the identification and authentication is successful, the user is allowed to use the TOE. If it fails, the user is not allowed to use it. However, regarding the viewing of the list of user job data, WIM Help, system status, counter, and information of inquiries, and execution of fax reception, the identification and authentication is not required for the use of the TOE.

FIA_USB.1

Based on the result of checking FIA_UAU.1 and FIA_UID.1, the TOE assigns the login user name, user role, and available function list to processes performed by the authorised user.

FIA_ATD.1

The TOE retains the login user name, user role, and available function list based on settings for each user. The privilege is set for each user according to the role to which the user is classified at the time of registration. The login user name assigned to the user can be changed for each user.

FTA_SSL.3

The TOE automatically logs out the users when they are logged in and do not operate the TOE for a certain period of time specified by the MFP administrator.
The TOE works as follows depending on the interface to which the user is logged-in.

- In case of the Operation Panel, the user is logged out of the TOE when the time that elapses since their final operation reaches the Operation Panel Auto Logout time (10 to 999 seconds).
- In case of the WIM, the user is logged out of the TOE when the time that elapses since their final operation reaches the WIM Auto Logout time (3 to 60 minutes).

The TOE also performs identification and authentication for the requests from the printer driver and the fax driver. At this time, there is no continuous interactive session that shall be automatically logged out because the user is logged out when the reception of the document data is completed.

FIA_UAU.7

Regarding login passwords entered by persons who attempt to use the Operation Panel or the WIM, the TOE does not display the entered letters, instead, it displays a sequence of dummy letters with same number of characters as the entered password on the login screen.

FIA_AFL.1

If the user enters a wrong password in succession when logging in, the lockout function will work and the TOE will prohibit the user from logging in with that login user name.

When the login fails due to entering a wrong password, the user is locked out when the number of attempts before lockout for the password (1 to 5 times) set by the MFP administrator is reached or exceeded.

The number of authentication failures is added up even if the login destination (Operation Panel, WIM, printer driver, and fax driver) varies.

With the locked-out login user name, authentication will fail even if the user enters the correct password. The user cannot use the TOE until the lockout is released after a certain period of time elapses or the MFP administrator or supervisor unlocks the lockout.

If a user name is locked out, the user with that user name is not allowed to log in unless any of the following conditions is fulfilled.

- For normal users, until the lockout time set by the MFP administrator elapses.
- For locked out users listed in Table 37, until an unlocking administrator specified for each user role releases the lockout.
- In case of the MFP administrator and supervisor, 60 seconds elapse since the MFP becomes executable after its power is turned off and then on.

Table 37 : Unlocking Administrators for Each User Role

User Role (Locked out User)	Unlocking Administrator
Normal user	MFP administrator
MFP administrator	Supervisor
Supervisor	MFP administrator

FIA_SOS.1

Login passwords for users can be registered only if these passwords meet the given conditions. Passwords cannot be registered if they do not satisfy the conditions.

Usable characters and character types are as follows. The password complexity, which determines the conditions for the number of combination of characters (two or more types, or three or more types) is set by the MFP administrator.

- Upper-case letters: [A-Z] (26 letters)
- Lower-case letters: [a-z] (26 letters)
- Numbers: [0-9] (ten digits)
- Symbols: SP (spaces) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ (33 symbols)

The conditions for registrable password length differ depending on normal users, MFP administrators, and a supervisor, as shown below. The minimum character number of login password (i.e. minimum password length) is set by the MFP administrator in the range of 8 to 32 characters.

- For normal users: Equal to or longer than the minimum password length, and 128 characters or less
- For MFP administrators and a supervisor: Equal to or longer than the minimum password length, and 32 characters or less

FPT_FDI_EXP.1

The TOE inputs information after the TSF reliably identifies and authenticates the input information from the Operation Panel or the client computer via LAN interface. Therefore, the input information cannot be forwarded unless the TSF is involved in information identification and authentication.

7.3 Document Access Control Function

The Document Access Control Function is to authorise the operations for document data and user job data by the authorised TOE users who are authenticated by Identification and Authentication Function. It allows user's operation on the document data and user job data based on the privileges for the user role, or the operation permissions for each user.

FDP_ACC.1(a) and FDP_ACF.1(a)

The TOE provides the Document Access Control Function by enforcing the user data access control SFPs.

Rules of user data access control SFP are divided into (1) access control rule on document data and (2) access control rule on user job data. According to them, the TOE restricts the operations on document data and user job data by users.

(1) Access control rule on document data

Table 38 describes the access control rules for document data. The TOE restricts the operation of deleting or reading document data to normal users, MFP administrators, and supervisors.

Table 39 describes normal user operations for document data, and Table 40 describes MFP administrator operations for document data. No interface is provided for the operations other than that described in Table 39 and Table 40.

Table 38 : Access Control Rules for Document Data

User Role	Document Data	Access Control Rule
Normal user	Document data (+PRT)	Normal users who have the same login user name as the login user name registered in the document owner information are allowed read and delete operations. For the read operation, other normal users cannot display the document data, and they are not allowed the read operation. For the delete operation, other normal users can display the jobs related to a temporary document data, but they are not allowed the delete operation.
	Document data (+CPY, +SCN, +FAXOUT)	Normal users who have the same login user name as the login user name registered in the document owner information are allowed read and delete operations. For the read operation, other normal users are not provided any interface for reading. For the delete operation, other normal users can display the jobs related to a temporary document data, but they are not allowed the delete operation.
	Document data (+FAXIN)	No interface for operating the fax reception data is provided.
	Document data (+DSR) (Stored print document, Document Server document, Scanned document, Fax transmission document)	Normal users who have the same login user name as the login user name registered in the document owner information are allowed read and delete operations. Also, normal users who have the same login user name as the login user name registered in the list for users who have been granted access permission for the document data are allowed the read operation. Other normal users cannot display the document data, and they are not allowed read and delete operations.
	Document data (+DSR) (Fax reception document)	Normal users who have the same login user name as the login user name registered in the document owner information (Stored Reception File User) are allowed read and delete operations. Other normal users cannot display the document data, and they are not allowed read and delete operations.

User Role	Document Data	Access Control Rule
MFP administrator	Document data (+PRT, +CPY, +SCN, +FAXOUT)	MFP administrators are allowed the delete operation for the document data.
	Document data (+FAXIN)	Fax reception (fax reception job) is regarded as reception by the MFP administrator, and the MFP administrator is allowed the read operation. No interface for deleting fax reception data is provided.
	Document data (+DSR) (Stored print document)	MFP administrators are allowed the delete operation for the document data.
	Document data (+DSR) (Document Server document, Scanned document, Fax transmission document)	MFP administrators are allowed read and delete operations for the document data.
	Document data (+DSR) (Fax reception document)	No interface for operating document data is provided.
Supervisor	Document data	No interface for operating document data is provided.

Table 39 : Normal User Operations for Document Data

No.	TOE Function (TOE Document Name)	Operation Path	Operations	SFR Package Functions in PP
1	Copy Function	Operation Panel	Delete (*1) Copy and print	F.CPY (+CPY)
2	Scanner Function	Operation Panel	Delete (*1) E-mail transmission of attachments Folder transmission Preview	F.SCN (+SCN)

No.	TOE Function (TOE Document Name)	Operation Path	Operations	SFR Package Functions in PP
3	Scanner Function (Scanned document)	Operation Panel	Delete E-mail transmission of attachments Folder transmission Preview	F.DSR (+DSR)
4	Fax Function	Operation Panel	Delete (*1) Fax transmission Preview	F.FAX (+FAXOUT)
5	Fax Function (Fax transmission document)	Operation Panel	Delete Fax transmission Preview	F.DSR (+DSR)
6	Fax Function (Fax reception document)	Operation Panel	Delete Print Preview	F.DSR (+DSR) F.PRT (+PRT)
7	Fax Function (Fax reception document)	WIM	Delete Download Preview	F.DSR (+DSR)
8	Printer Function (Temporary saved document)	Operation Panel	Delete (*1) Print Preview	F.PRT (+PRT)
9	Printer Function (Temporary saved document)	WIM	Delete (*1)	F.PRT (+PRT)
10	Printer Function (Stored print document)	Operation Panel	Delete Print Preview	F.DSR (+DSR) F.PRT (+PRT)
11	Printer Function (Stored print document)	WIM	Delete	F.DSR (+DSR)

No.	TOE Function (TOE Document Name)	Operation Path	Operations	SFR Package Functions in PP
12	Document Server Function (Fax transmission document, Document Server document)	Operation Panel	Delete Print Preview	F.DSR (+DSR) F.PRT (+PRT)
13	Document Server Function (Scanned document)	WIM	Delete E-mail transmission of attachments Folder transmission Download Preview	F.DSR (+DSR)
14	Document Server Function (Fax transmission document)	WIM	Delete Fax transmission Download Preview	F.DSR (+DSR)
15	Document Server Function (Document Server document)	WIM	Delete Preview	F.DSR (+DSR)

(*1) By cancelling the job, the temporary document data handled by the user job data will be deleted.

Table 40 : MFP Administrator Operations for Document Data

No.	TOE Function (TOE Document)	Operation Path	Operations	SFR Package Functions in PP
1	Copy Function	Operation Panel	Delete (*1)	F.CPY (+CPY)
2	Scanner Function	Operation Panel	Delete (*1)	F.SCN (+SCN)
3	Scanner Function (Scanned document)	Operation Panel	Delete	F.DSR (+DSR)
4	Fax Function	Operation Panel	Delete (*1)	F.FAX (+FAXOUT)

No.	TOE Function (TOE Document)	Operation Path	Operations	SFR Package Functions in PP
5	Printer Function (Temporary saved document)	Operation Panel	Delete (*1)	F.PRT (+PRT)
6	Printer Function (Temporary saved document)	WIM	Delete (*1)	F.PRT (+PRT)
7	Printer Function (Stored print document)	Operation Panel	Delete	F.DSR (+DSR)
8	Printer Function (Stored print document)	WIM	Delete	F.DSR (+DSR)
9	Document Server Function (Fax transmission document, Document Server document)	Operation Panel	Delete	F.DSR (+DSR)
10	Document Server Function (Scanned document, Fax transmission document, Document Server document)	WIM	Delete Preview	F.DSR (+DSR)

(*1) By cancelling the job, the temporary document data handled by the user job data will be deleted.

(2) Access control rule on user job data

The TOE provides users with the interface for deleting user job data (cancelling the job). However, no interface for deleting user job data for fax reception (+FAXIN) is provided.

No interface for modifying the user job data is provided.

- For normal user: The normal user whose login user name matches the login user name registered in the user job data owner information is allowed to delete the user job data. Other normal users are allowed to display the user job data, but are not allowed to delete the user job data.

- For MFP administrator: MFP administrators are allowed to delete the user job data.
- For supervisor: No interface for operating the user job data is provided.

7.4 Use-of-Feature Restriction Function

The Use-of-Feature Restriction Function is to authorise the job execution of MFP applications based on the roles of authorised users who are identified and authenticated and the operation permissions for each user.

FDP_ACC.1(b) and FDP_ACF.1(b)

The TOE provides the Use-of-Feature Restriction Function by enforcing the TOE function access control SFP that determines whether the job execution of MFP applications provided by the TOE is authorised for normal users and the additional rules for MFP administrators and a supervisor.

The TOE verifies the role for an authorised user who attempts to start executing the job of MFP applications (Copy Function, Printer Function, Scanner Function, Document Server Function, and Fax Function) provided by the TOE. If the user role is normal user, only the job execution for the MFP applications whose function type matches those in available function list is permitted. If the user role is MFP administrator, the job execution for MFP applications is permitted. If the user role is supervisor, the job execution for MFP applications is not permitted.

7.5 Stored Data Protection Function

The Stored Data Protection Function is to encrypt data to be written to the HDD in order to protect data recorded in the HDD from data leakage.

FCS_CKM.1

The TOE generates a 256-bit HDD cryptographic key using the CTR_DRBG (AES-128) algorithm when encrypting the HDD upon operation by the MFP administrator.

At this time, the TOE generates random numbers using an algorithm that is compliant with the standard NIST SP 800-90A.

FCS_CKM.4

When decrypting the HDD, the cryptographic key is overwritten with 0.

FCS_COP.1

The TOE encrypts the data to be written to the HDD before writing it and decrypts the data to be read from the HDD after reading it. The TOE conforms to the standard FIPS197, and encrypts and decrypts data using the AES algorithm with a key of 256-bit cryptographic key size.

7.6 Network Protection Function

The Network Protection Function is to prevent information leakage due to network monitoring and detect alteration by providing encrypted communication when communicating with trusted IT products. Communication with the client computer when using WIM, printer driver, or fax driver is encrypted by TLS, and communication with SMB server and FTP server when using folder transmission is protected by IPsec. Also, communication with mail server when using e-mail transmission of attachments is protected by S/MIME, and communication with syslog server when the audit log transfer setting is enabled is encrypted by TLS.

FTP_ITC.1

The TOE provides different encrypted communications depending on communicating devices when the TOE communicates with trusted IT products (WIM communication, folder transmission, e-mail transmission of attachments, temporary saving or storing document data received from the printer driver, storing document data received from the fax driver, and transfer to the syslog server). The TOE allows the client computer's Web browser, printer driver, or fax driver to initiate encrypted communication. The TOE can initiate encrypted communication with the mail server, SMB server, FTP server, or syslog server. Table 41 describes the encrypted communications provided by the TOE.

When using the WIM, encrypted communication with the client computer is performed by specifying a URL for which encrypted communication is valid on a Web browser. When using the Printer Function, encrypted communication with the client computer (IPP over SSL) is performed when document data is sent from the printer driver to the TOE. When using the Fax Function, encrypted communication with the client computer (IPP over SSL) is performed when document data is sent from the fax driver to the TOE. When using the e-mail transmission of attachments, encrypted communication with the mail server (S/MIME) is performed. When using the folder transmission, encrypted communication with the FTP server or SMB server (IPsec) is performed. When using the syslog transfer function, encrypted communication with the syslog server protected by TLS is performed by using the syslog protocol.

Table 41 : Encrypted Communications Provided by the TOE

Communicating Device	Encrypted Communication Provided by the TOE	
	Protocol	Cryptographic Algorithms
Client computer (*1)	TLS1.2	AES (128 bits, 256 bits)
	TLS1.3	AES (128 bits, 256 bits), ChaCha20 (256 bits)
FTP server	IPsec	AES (128 bits, 192 bits, 256 bits)
SMB server	IPsec	AES (128 bits, 192 bits, 256 bits)
Mail server	S/MIME	AES (128 bits, 256 bits)
syslog server	TLS1.2	AES (128 bits, 256 bits)
	TLS1.3	AES (128 bits, 256 bits), ChaCha20 (256 bits)

(*1) When the communication uses the printer driver or fax driver, the TLS version of the supporting protocol depends on the OS version of the client computer.

7.7 Residual Data Overwrite Function

The Residual Data Overwrite Function is to overwrite random numbers or specific pattern data on the HDD and disable the reusing of the residual data included in deleted document data, temporary document data and their fragments on the HDD.

FDP_RIP.1

Methods to delete the HDD area through overwriting include sequential overwriting and batch overwriting.

For sequential overwriting, the TOE constantly monitors the information on a residual data area, and overwrites the area if any existing residual data is discovered. When the user deletes document data, the TOE overwrites the area on the HDD where the digital image data of the document data is stored with random numbers. Also, when the job is complete, the TOE overwrites the area on the HDD where temporary document data that are created while the job is executed or the fragments of those temporary document data are stored with random numbers.

For batch overwriting, the TOE collectively overwrites the HDD. The TOE overwrites the HDD with the method specified by the MFP administrator. Batch overwriting methods include NSA, DoD, random number, BSI/VSITR, and Secure Erase methods.

The NSA method overwrites twice with random numbers and once with Null(0). The DoD method overwrites once with a certain value, once with its complement, and further with random numbers to be verified afterwards. The random number method overwrites three to nine times with random numbers. The MFP administrator specifies the number of times to overwrite when the TOE is installed. The BSI/VSITR method overwrites data with 00, FF, 00, FF, 00, FF, AA in this order. The Secure Erase method overwrites data using the ATA command "secure erase".

7.8 Security Management Function

The Security Management Function is to control operations for TSF data in accordance with user privileges allocated to each user or user role privileges allocated to the normal user, MFP administrator, and supervisor. In order to enable control, this function includes a function to maintain the user role of operating the Security Management Function and associate the user role with the authorised TOE user authenticated by the Identification and Authentication Function, and a function to set appropriate default values for the security attributes.

FMT_SMR.1

The TOE user has the role of normal user, MFP administrator, or supervisor. The role is associated with the login user name registered in the TOE. The TOE associates the logged-in user with the role corresponding to the login user name.

FMT_SMF.1, FMT_MOF.1, FMT_MSA.1(a), FMT_MSA.1(b), FMT_MTD.1(a), and FMT_MTD.1(b)

The TOE performs the following management functions:

- The TOE provides only the MFP administrators with an interface for setting the syslog transfer function to stop or operate.

- The TOE restricts operations on the TSF data according to the role of the user. As shown in Table 42, it allows users who have privilege corresponding to the role for which operations are allowed to operate the TSF Data.

Table 42 : Management of TSF Data

Category	TSF Data	Operations	User Role with Operation Permission	Operation Interface
TSF protected data	Lockout settings	Modify	MFP administrator	WIM
	Date/time settings	Modify	MFP administrator	Operation Panel WIM
	Password quality settings	Modify	MFP administrator	Operation Panel WIM
	Auto Logout settings	Modify	MFP administrator	Operation Panel WIM
	S/MIME user information	Newly create Modify Delete	MFP administrator	Operation Panel (*3) WIM
	Destination folder	Newly create Modify Delete	MFP administrator	Operation Panel WIM
	Audit log settings	Modify	MFP administrator	Operation Panel WIM
	Cryptographic communication settings	Modify	MFP administrator	Operation Panel WIM
	Login user name [When associated with a normal user]	Newly create Modify Delete	MFP administrator	Operation Panel WIM
	Login user name [When associated with an MFP administrator]	Newly create	MFP administrator	Operation Panel WIM
		Modify	MFP administrator in question	
	Login user name [When associated with a supervisor]	Modify	Supervisor	Operation Panel WIM
	User role	Modify (*1)	None	None
	Document data owner information [+PRT, +SCN, +FAXIN, +FAXOUT, +CPY]	Modify (*1)	None	None
	Document data owner information [Other than +DSR and Fax reception document]	Modify (*1)	None	None

Category	TSF Data	Operations	User Role with Operation Permission	Operation Interface
	Document data owner information [+DSR, Fax reception document]	Modify	MFP administrator	Operation Panel WIM
	List for users who have been granted access permission for the document data	Modify	MFP administrator Document data owner (Normal user)	Operation Panel (*4) WIM
		Change_default	MFP administrator	Operation Panel WIM
	User job data owner information	Modify (*1)	None	None
	Available function list	Newly create Modify Delete	MFP administrator	Operation Panel WIM
	Function type	Modify (*1)	None	None
TSF confidential data	Login password [When associated with a normal user]	Newly create	MFP administrator	Operation Panel WIM
		Modify	Normal user in question MFP administrator	
		Query (*2)	None	
	Login password [When associated with an MFP administrator]	Newly create	MFP administrator	Operation Panel WIM
		Modify	MFP administrator in question Supervisor	
		Query (*2)	None	
	Login password [When associated with a supervisor]	Modify	Supervisor	Operation Panel WIM
		Query (*2)	None	
	HDD cryptographic key	Query Delete Newly create	MFP administrator	Operation Panel

(*1) No interface is provided for modification.

(*2) No interface is provided for query.

(*3) The operation that can be performed from the Operation Panel is only the operation of the e-mail addresses that is the item set for each user, included in the S/MIME user information.

(*4) For Stored print document, the list for users who have been granted access permission for the document data cannot be operated by using the Operation Panel. It can be operated only by using WIM.

FMT_MSA.3(a) and FMT_MSA.3(b)

Table 43 describes the list of static initialisation for security attributes, and Table 44 describes security attributes for each case of document data generation.

The TOE sets default values of security attributes for objects according to the rules described in Table 43 and Table 44 when those objects are generated. Overwriting the default values of the security attributes is allowed only in limited cases, and "None" is indicated when no overwriting interface is provided.

Table 43 : List of Static Initialisation for Security Attributes

Object	Security Attribute	Default Value	Overwriting Default Value
Document data	Document data owner information	See Table 44.	See Table 44.
	List for users who have been granted access permission for the document data	See Table 44.	See Table 44.
User job data	User job data owner information	Login user names of normal users who created the user job data.	None
MFP application	Function type	Values that identify each function (Copy Function, Scanner Function, Printer Function, Fax Function, and Document Server Function) among the MFP applications.	None

Table 44 : Security Attributes for Each Case of Document Data Generation

Case of Document Data Generation	Security Attribute	Default Value	Overwriting Default Value
Scans a paper document, and then copies and prints scanned image data from the Operation Panel by using the Copy Function (F.CPY)	Document data owner information	Login user names of normal users who created the document data.	None
Scans a paper document and performs folder transmission or e-mail transmission of attachments from the Operation Panel by using the Scanner Function (F.SCN)	Document data owner information	Login user names of normal users who created the document data.	None

Case of Document Data Generation	Security Attribute	Default Value	Overwriting Default Value
Scans a paper document and performs fax transmission from the Operation Panel by using the Fax Function (F.FAX)	Document data owner information	Login user names of normal users who created the document data.	None
Receives the document data and temporarily saves it in the TOE from the printer driver by using the Printer Function (F.PRT)	Document data owner information	Login user names of normal users who created the document data.	None
Receives the document data via a telephone line by using the Fax Function (F.FAX)	None	None	None
Receives the document data via a telephone line and stores it by using the Fax Function (F.DSR)	Document data owner information	The list that fax reception document owner information (the login user names) is set (Stored Reception File User)	None
Scans a paper document and stores it from the Operation Panel by using the Scanner Function (F.SCN and F.DSR)	Document data owner information	Login user names of normal users who created the document data.	None
	List for users who have been granted access permission for the document data	Default values in the list for users who have been granted access permission for the document data (the list of login user names) for the document data creator	The values that the document data creator has allowed access (viewing) (the list of login user names) can be overwritten from the Operation Panel.
Scans a paper document and stores it from the Operation Panel by using the Fax Function (F.SCN and F.DSR)	Document data owner information	Login user names of normal users who created the document data.	None
	List for users who have been granted access permission for the document data	Default values in the list for users who have been granted access permission for the document data (the list of login user names) for the document data creator	The values that the document data creator has allowed access (viewing) (the list of login user names) can be overwritten from the Operation Panel.
Receives the document data and stores it from the fax	Document data owner information	Login user names of normal users who created the document data.	None

Case of Document Data Generation	Security Attribute	Default Value	Overwriting Default Value
driver by using the Fax Function (F.DSR)	List for users who have been granted access permission for the document data	Default values in the list for users who have been granted access permission for the document data (the list of login user names) for the document data creator	None
Scans a paper document and stores it from the Operation Panel by using the Document Server Function (F.SCN and F.DSR), or scans a paper document and stores it by using the Copy Function (F.SCN and F.DSR)	Document data owner information	Login user names of normal users who created the document data.	None
	List for users who have been granted access permission for the document data	Default values in the list for users who have been granted access permission for the document data (the list of login user names) for the document data creator	The values that the document data creator has allowed access (viewing) (the list of login user names) can be overwritten from the Operation Panel.
Receives the document data and stores it from the printer driver specifying the print method as Document Server storage or stored print by using the Printer Function (F.DSR)	Document data owner information	Login user names of normal users who created the document data.	None
	List for users who have been granted access permission for the document data	Default values in the list for users who have been granted access permission for the document data (the list of login user names) for the document data creator	None

7.9 Integrity Verification Function

The Integrity Verification Function is a self-test function to verify that a part of TSF and the TSF executable code have a software configuration that maintains integrity during the MFP initial start-up. The objects whose integrity is verified here are the executable codes of the MFP Control Software and Operation Panel Control Software, and HDD cryptographic keys.

FPT_TST.1

The TOE verifies the integrity of the Operation Panel Control Software during the initial start-up by comparing the hash value of the Operation Panel Control Software with the correct value or verifying the signature. If the obtained hash value does not match the correct value, or if the signature is not verified, the TOE will display an error message on the Operation Panel and will not accept the operation.

The TOE verifies the integrity of the MFP Control Software during the initial start-up by comparing the hash value with the correct value or verifying the signature. If the obtained hash value does not match the correct value, or if the signature is not verified, the TOE will display an error message on the Operation Panel and will

not accept the operation. The hash-verified part of the MFP Control Software is verified, and then the integrity of the HDD cryptographic key is verified. If the hash value obtained from the HDD cryptographic key does not match the correct value, the TOE will display an error message on the Operation Panel and will not accept the operation. If the hash value obtained from the HDD cryptographic key matches the correct value, the TOE will perform verification using the signature of the MFP Control Software. If the obtained hash value does not match the correct value, or if the signature is not verified, the TOE will display an error message on the Operation Panel and will not accept the operation.

If the hash values obtained from the Operation Panel Control Software and the MFP Control Software match the correct values, and if the signature is verified, the TOE becomes available.

7.10 Fax Line Separation Function

The Fax Line Separation Function is to restrict the input information from the telephone line to only fax reception and prohibit forwarding of received fax data in order to prevent unauthorised intrusion into the LAN from the telephone line.

FPT_FDI_EXP.1

The TOE restricts the input information from the telephone line so that only fax data can be received. If any communication that does not comply with the fax protocol with the G3 standard is performed, the line is disconnected. Since the TOE is set to prohibit forwarding of received fax data when the TOE is installed, received fax data will not be forwarded.

8 Glossary

In this section, the meanings of specific terms used in this ST are defined below.

Table 45 : Specific Terms Related to This ST

Term	Definition
Lockout	A type of behaviour to deny login of particular users.
Auto Logout function	A function for automatic user logout if no access is attempted from the Operation Panel or the WIM for the predetermined period of time. Also called Auto Logout.
HDD	An abbreviation of hard disk drive. In this document, unless otherwise specified, "HDD" indicates the HDD installed on the TOE.
Job	A sequence of operations of each TOE function (Copy Function, Scanner Function, Printer Function, Document Server Function, Fax Transmission Function, and Fax Reception Function) from beginning to end.
MFP application	General term for Copy Function, Printer Function, Scanner Function, Fax Function, and Document Server Function enforcing F.CPY, F.PRT, F.SCN, F.FAX, and F.DSR.
Copy Function	One of the MFP applications. It enforces the SFR package functions for F.CPY and F.DSR.
Scanner Function	One of the MFP applications. It enforces the SFR package functions for F.SCN and F.DSR.
Printer Function	One of the MFP applications. It enforces the SFR package functions for F.PRT and F.DSR.
Fax Function	One of the MFP applications. It enforces the SFR package functions for F.FAX and F.DSR.
Document Server Function	One of the MFP applications. It enforces the SFR package function for F.DSR.
Temporary saved document	The document data received from the printer driver by specifying the print method that is handled as temporary saving and temporarily saved in the TOE. The document data attribute corresponds to +PRT.
Stored print document	Among the document data stored in the TOE, it refers to the document data that is received and stored by specifying the print method as stored print from the printer driver. The document data attribute corresponds to +DSR.
Document Server document	Among the document data stored in the TOE, it refers to the document data that is stored in the TOE after scanning paper documents from the Operation Panel by using the Copy Function or the Document Server Function, and the document data that is received from the printer driver by specifying the print method as Document Server storage. The document data attribute corresponds to +DSR.
Scanned document	Among the document data stored in the TOE, it refers to the document data that is stored after scanning paper documents from the Operation Panel by using the Scanner Function. The document data attribute corresponds to +DSR.

Term	Definition
Fax transmission document	Among the document data stored in the TOE, it refers to the document data that is stored after scanning paper documents from the Operation Panel by using the Fax Function, and the document data that is received and stored from the fax driver. The document data attribute corresponds to +DSR.
Fax reception document	Among the document data stored in the TOE, it refers to the document data that is received from the external fax via a telephone line and stored in the TOE. The document data attribute corresponds to +DSR.
Stored Reception File User	A list that is set with the owner information (the login user names) of fax reception documents. There is one list for all fax reception documents.
Operation Panel	A unit that consists of a LCD touch screen and key switches. The Operation Panel is used by users to operate the TOE.
WIM	Web Image Monitor function. This is a function for TOE users to remotely operate the TOE from the client computer's Web browser.
Folder transmission	A function that scans paper documents from the Operation Panel by using the Scanner Function and then sends scanned image data or stored scanned document from the MFP via networks to a shared folder in an SMB server by using SMB protocol, or sends document data to a folder in an FTP server by using FTP protocol. IPsec protects the communication for enforcing this function.
E-mail transmission of attachments	A function that scans paper documents from the Operation Panel by using the Scanner Function and then sends scanned image data or the stored scanned document in e-mail format. S/MIME protects the communication for enforcing this function.
SPDF	A type of Auto Document Feeder (ADF) that feeds the originals set on the device one by one to the exposure glass. When scanning both sides of the original, both sides are scanned simultaneously.
TOE owner	An individual or organisation indirectly involved with the TOE and is responsible for protecting the TOE assets and establishing related security policies.