RICOH IM 460F/370F

Security Target

Author:	RICOH COMPANY, LTD.
Date:	2024-02-16
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 the ST.

Title: RICOH IM 460F/370F Security Target

Version: 1.00

Date: 2024-02-16

Author: RICOH COMPANY, LTD.

1.2 TOE Reference

The following is the identification information of the TOE.

TOE Names: RICOH IM 460F/370F

Version: J-1.00

TOE Type: Multifunction product (hereinafter "MFP")

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

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

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

Table 2 describes the identification information of version and part number of software 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 2: 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

No.	Name of Software for the MFP	Version	Part Number
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
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

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

No.	Name of Software for the Operation Panel Unit	Version	Part Number
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
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 describes TOE Type, TOE Usage, and Major Security Features 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 Features of the 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, eMMC encryption, and encrypted communication are provided to prevent disclosure or alteration of assets, including document data processed by the TOE and setting information related to security functions, through unauthorized 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. Since the TOE is not equipped with an HDD and processes user data with an eMMC, the Residual Data Overwrite Function is not included in the security functions to be evaluated.

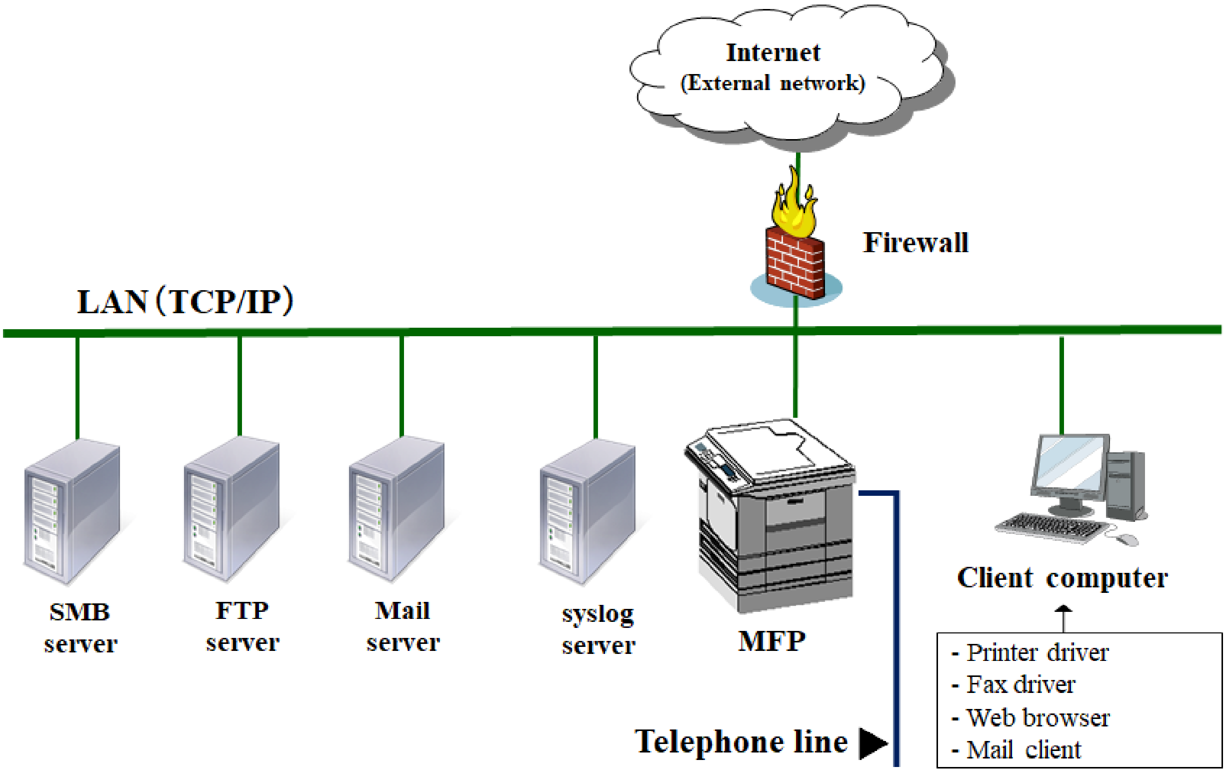


Figure 1: Example of TOE Environment

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 or later version) 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 or later version) 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 unauthorized 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 Physical Boundary of the TOE and Logical Boundary of the TOE.

1.4.1 Physical Boundary of the TOE

The TOE consists of the MFP products in Table 1 and guidance documents in Table 4. The target MFP product is the one equipped with software of a TOE version (J-1.00) listed in Table 3.

A delivery company delivers the MFP to users.

A guidance set of [Japanese Version 1] will be delivered. Some guidance documents are included in the MFP, and others are delivered through the Web.

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

Table 3: Combination to Be Delivered

No.	MFP			Guidance Document	Remarks
	Product Name	Model Code	Version		
1	RICOH IM 460F	D0DN-00	J-1.00	[Japanese Version-1]	SPDF is installed as standard
2	RICOH IM 370F	D0DM-03	J-1.00	[Japanese Version-1]	SPDF is installed as standard

Table 4 describes guidance documents, formats, and delivery methods for the guidance document set of [Japanese Version 1].

Table 4: Guidance Documents for [Japanese Version 1]

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-7304 2023.11.10	使用説明書<Common Criteria 準拠でお使いになる管理者の方へ>	PDF	Through the Web

No.	Part Number	Guidance Document Name	Format	Delivery Method
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-eal2-spf/ja/Guidance_ja.zip

Hash value (SHA256): d6d33162a728846622d465ad6ede9250edd1e8f51bba3a484f13467b67e4029d

1.4.2 Logical Boundary of the TOE

The logical boundary of the TOE is described below.

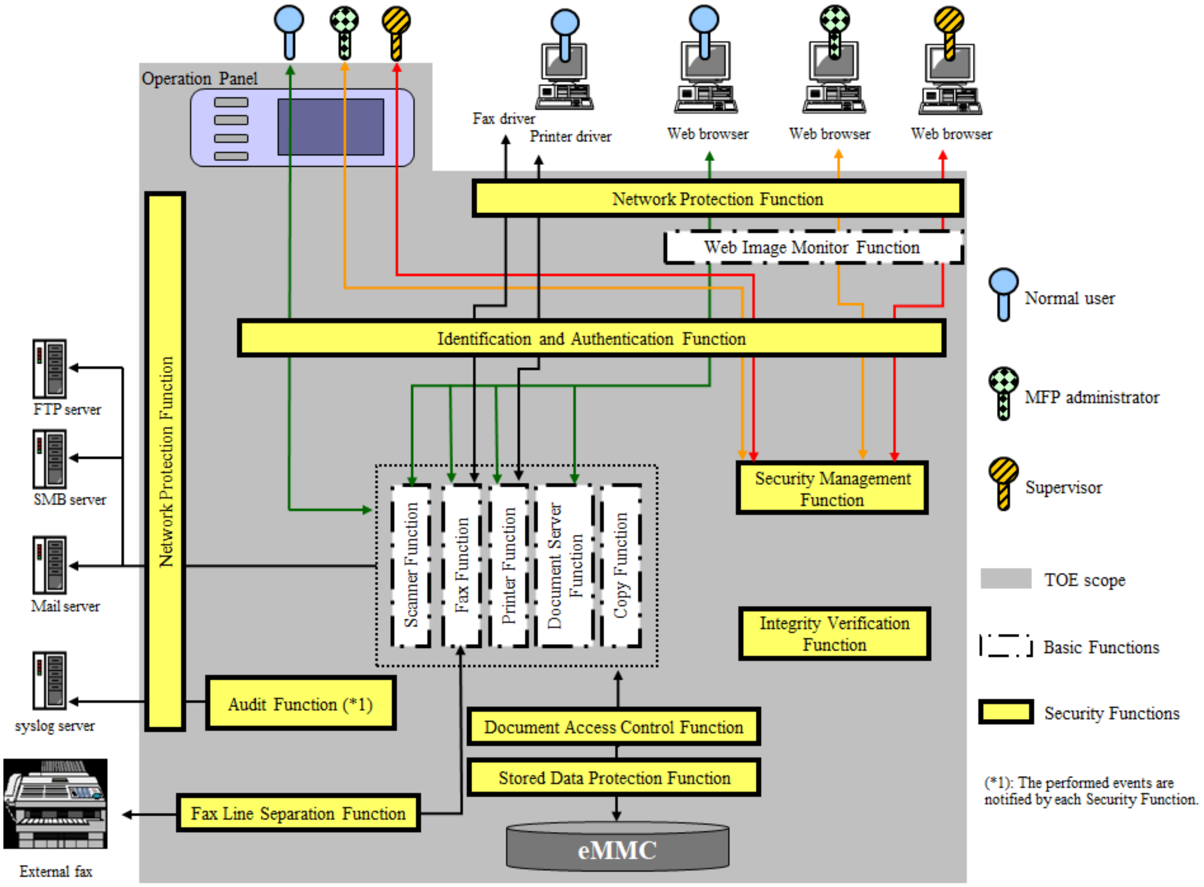

Operation Panel
Fax driver
Printer driver
Web browser
Web browser
Web browser
Network Protection Function
Web Image Monitor Function
Identification and Authentication Function
Network Protection Function
FTP server
SMB server
Mail server
syslog server
External fax
Scanner Function
Fax Function
Printer Function
Document Server Function
Copy Function
Security Management Function
Integrity Verification Function
Audit Function (*1)
Document Access Control Function
Stored Data Protection Function
Fax Line Separation Function
eMMC
Normal user
MFP administrator
Supervisor
TOE scope
Basic Functions
Security Functions
(*1): The performed events are notified by each Security Function.

Figure 2: Logical Boundary of the TOE

As shown in Figure 2, the TOE has Basic Functions and Security Functions, which of each are described below.

1.4.2.1. Basic Functions

The overview of the Basic Functions is described below.

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. Also, image to be copied and printed can be stored in the TOE. 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 has a function to temporarily save document data received from the printer driver by specifying the 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 temporarily-saved document data.

When the print method is specified as stored print in the printer driver, 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 deleted from the Web browser as a stored print document.

When the print method is specified as Document Server storage in the printer driver, document data can be stored in the TOE from the printer driver. 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 scanned image of the paper document from the Operation Panel can be stored in the TOE. 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. 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 a scanned image of a paper document as document data to external fax devices from the Operation Panel.

Also, the scanned image of the paper document from the Operation Panel can be stored in the TOE, 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. 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, and then store it in the TOE. 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.

Document Server Function

The Document Server Function stores a scanned image of a paper document in the TOE from the Operation Panel. 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. For document data stored in the TOE by using functions other than the Document Server Function, the following operations can also be performed.

- 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 Functions

The Security Functions are described below.

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 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 file to append the newest audit log. The TOE can also 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 user data. 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.

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.

Stored Data Protection Function

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

Security Management Function

The Security Management Function is to control operations for TSF data in accordance with privileges allocated to each user or role privileges allocated to the normal user, MFP administrator, and supervisor. In order to enable control, this function includes a function to maintain the role of operating the Security Management Function and associate the 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 that verifies the integrity of executable code in the TSF.

Fax Line Separation Function

The Fax Line Separation Function is to prohibit communication via a fax interface, except for transmission or reception of user data using a fax protocol, in order to prevent intrusion from the telephone line (same meaning as Fax Line in this function name) into the LAN.

2 Conformance Claim

This section describes Conformance Claim.

2.1 CC Conformance Claim

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

- CC version for which this ST and the 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

There is no PP that this ST and TOE conform to.

2.3 Package Claims

This ST and TOE claim conformity to package: EAL2.

There are no assurance components to be added.

2.4 Conformance Claim Rationale

This ST and TOE do not claim PP conformity.

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 administrators are divided into MFP administrators and supervisors.

As described in Table 5, the users are classified according to their respective roles, and have user privileges based on the roles of normal users, MFP administrators, and supervisors.

Table 5: Definition of Users

Definition of Users		Explanation
Normal user		A user who is allowed to use the TOE. A normal user is provided with a login user name and can operate user data.
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 documents - Unlocking locked-out normal users and 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 and TSF data. The definitions are described in Table 6.

Table 6: Asset Categories

Category	Definition
User data	Data created by the user, for the user, that does not affect the operation of the TSF.
TSF data	Data created by the TOE, for the TOE, that may affect the operation of the TSF.

3.2.1 User Data

The user data is categorized into document data and user job data. .The category definitions are described in Table 7.

Table 7: Definitions of User Data

Category	Definition
Document data	Information contained in the user's document in electronic or hard-copy format. Document data stored and saved in the eMMC (stored document data) and document data received from the printer driver and temporarily saved in the TOE (temporarily-saved document) are included. Stored document data includes scanned documents, fax transmission documents, fax reception documents, stored print documents, and Document Server documents.
User job data	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. The category definitions are described in Table 8.

Table 8: TSF Data Categories

TSF Data Category	Definition
TSF protected data	Protected TSF data that does not pose a security threat when published, but must be protected from unauthorised alteration.
TSF confidential data	Confidential TSF data that must be protected so that it cannot be viewed or modified by anyone other than authorised users.

The TSF data handled by this TOE for each category is described below.

Table 9: Definitions of TSF Data

Category	TSF Data	Description
TSF protected data	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.

Category	TSF Data	Description
	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 communications with clients and servers.
	Login user name	User identifier associated with any of the normal user, MFP administrator, and supervisor. The TOE identifies users by this identifier.
	User privilege	Any role of normal user, MFP administrator, or supervisor who uses the TOE, and the privilege according to that role.
	Document data owner information	The security attribute of document data (temporarily-saved document data, scanned documents, fax transmission documents, stored print documents, and Document Server documents). The owner information (the login user name) of document data (except fax reception documents) is set.
	List of users who have been granted access permission for the document data	The security attribute of document data (temporarily-saved document data, scanned documents, fax transmission documents, stored print documents, and Document Server documents). The information of users (the login user names) who are allowed access (viewing) document data (except fax reception documents) is set. The document data owner can allow other normal users to read the document data.
	Fax reception document user	The security attribute of fax reception documents. The list of the login user names of users who have been granted access (read and delete) permission for fax reception documents is set. The users are managed with one list for all fax reception documents.
	User job data owner information	The security attribute of user job data. The information of user job data owners (the login user name) is set.
TSF confidential data	Login password	A password associated with each login user name.
	Audit log	Audit log data in which events occurred are recorded.
	eMMC cryptographic key	Cryptographic key used to encrypt data in the eMMC.

3.3 Threats

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

T.DOCUMENT_DATA_DIS **Disclosure of document data**

Document data under the TOE management may be disclosed by persons without a login user name, or by persons with a login user name but without an access permission to the document data.

T.DOCUMENT_DATA_ALT **Alteration of document data**

Document data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the document data.

T. JOB_ALT **Alteration of user job data**

User job data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the user job data.

T.PROTECT_DATA_ALT **Alteration of TSF protected data**

TSF protected data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the TSF protected data.

T.CONFIDENTIAL_DATA_DIS **Disclosure of TSF confidential data**

TSF confidential data under the TOE management may be disclosed by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

T.CONFIDENTIAL_DATA_ALT **Alteration of TSF confidential data**

TSF confidential data under the TOE management may be altered by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

3.4 Organisational Security Policies

The following organisational security policies are taken as matters to be complied by TOE: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 created by the National Institute of Standards and Technology is considered.

P.AUTHORIZATION **User identification and authentication**

Only users with operation permission of the TOE shall be authorised to use the TOE.

P.VALIDATION **Software verification**

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

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

To maintain operational accountability and security, records that provide an audit trail of TOE security-relevant events shall be created, maintained, protected from disclosure and alteration by unauthorised persons, and confirmed by authorised persons.

P.FAX **Management of external interfaces**

For provision of the Fax Function over the telephone line by the TOE, the separation between the telephone line and the LAN shall be ensured.

P.ENCRYPTION **eMMC encryption**

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

3.5 Assumptions

This section identifies and describes the assumptions related to the operational environment of this TOE.

A.PHYSICAL_PROTECTION **Access management**

The MFP administrator shall install the TOE in a secure and monitored area in accordance with the guidance documents and restrict a chance of physical access by unspecified number of persons.

A.NETWORK_PROTECTION **Network management**

The MFP administrator shall install the TOE in an operational environment protected from any external attempt to directly access the TOE's LAN interfaces.

A.USER **User training**

The MFP administrator shall train normal users according to the guidance documents and ensure that normal users are aware of the security policies and procedures of their organisation and have the competence to follow those policies and procedures.

A.ADMIN **Administrator training**

The MFP administrator shall be aware of the security policies and procedures of their organisation and have the competence to correctly configure and operate the TOE in accordance with the guidance documents following those policies and procedures.

A.TRUSTED_ADMIN **Trusted administrator**

Persons who do not use their privileged access rights for malicious purposes according to the guidance documents shall be appointed as administrators.

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.DOCUMENT_DATA_DIS **Protection of document data disclosure**

The TOE shall protect document data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the document data.

O.DOCUMENT_DATA_ALT **Protection of document data alteration**

The TOE shall protect document data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the document data.

O.JOB_ALT **Protection of user job data alteration**

The TOE shall protect user job data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the user job data.

O.PROTECT_DATA_ALT **Protection of TSF protected data alteration**

The TOE shall protect TSF protected data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF protected data.

O.CONFIDENTIAL_DATA_DIS **Protection of TSF confidential data disclosure**

The TOE shall protect TSF confidential data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

O.CONFIDENTIAL_DATA_ALT **Protection of TSF confidential data alteration**

The TOE shall protect TSF confidential data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

O.AUTHORIZATION **User identification and authentication**

The TOE shall require identification and authentication of users and shall ensure that users are authorised in accordance with security policies before allowing them to use the TOE.

O.FAX **Management of external interfaces by TOE**

For provision of the Fax Function over the telephone line by the TOE, the TOE shall ensure the separation between the telephone line and the LAN.

O.VALIDATION **Software verification**

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

O.AUDIT **Management of audit log records**

The TOE shall ensure that logs of TOE security-relevant events are created and maintained as audit log, and protected from disclosure or alteration by unauthorised persons. It shall also provide audit logs in a format that can be verified by authorised persons.

O.EMMC_ENCRYPTION **eMMC encryption**

The TOE shall ensure that the function to encrypt data first and then store it in the eMMC is provided.

4.2 Security Objectives for Operational Environment

This section describes the security objectives for the operational environment.

OE.AUDIT **Audit log protection in trusted IT products**

The MFP administrator shall ensure that audit logs that are exported to a trusted IT product are protected from unauthorised access and modifications.

OE.PHYSICAL_PROTECTION **Physical management**

The MFP administrator shall ensure that the TOE is installed in a secure and monitored area in accordance with the guidance documents and a chance of physical access by unspecified number of persons is restricted.

OE.NETWORK_PROTECTION **Network management**

The MFP administrator shall ensure that the TOE is installed in an operational environment protected from any external attempt to directly access the TOE's LAN interfaces.

OE.AUTHORIZED_USER **Assignment of user authority**

The MFP administrator shall give users the authority to use the TOE in accordance with the security policies and procedures of their organisation.

OE.TRAINED_USER **User training**

The MFP administrator shall train users according to the guidance documents and ensure that users are aware of the security policies and procedures of their organisation and have the competence to follow those policies and procedures.

OE.TRAINED_ADMIN **Administrator training**

The responsible manager of MFP shall ensure that MFP administrators are trained to correctly configure and operate the TOE in accordance with the guidance documents following the security policies and procedures of their organisation and they have the competence to follow those policies and procedures.

OE.TRUSTED_ADMIN **Trusted administrator**

The responsible manager of MFP shall appoint administrators who will not use their privileged access rights for malicious purposes according to the guidance documents.

OE.AUDIT_MANAGE **Log audit**

The MFP administrator 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 10 describes the correspondence between the assumptions, threats and organisational security policies, and each security objective.

Table 10: Rationale for Security Objectives

Security Objectives Security Problem Definitions	O.DOCUMENT_DATA_DIS	O.DOCUMENT_DATA_ALT	O.JOB_ALT	O.PROTECT_DATA_ALT	O.CONFIDENTIAL_DATA_DIS	O.CONFIDENTIAL_DATA_ALT	O.AUTHORIZATION	OE.AUTHORIZED_USER	O.VALIDATION	O.AUDIT	OE.AUDIT	OE.AUDIT_MANAGE	O.FAX	OE.PHYSICAL_PROTECTION	OE.NETWORK_PROTECTION	O.EMMC_ENCRYPTION	OE.TRAINED_ADMIN	OE.TRUSTED_ADMIN	OE.TRAINED_USER
T.DOCUMENT_DATA_DIS	X						X	X											
T.DOCUMENT_DATA_ALT		X					X	X											
T.JOB_ALT			X				X	X											
T.PROTECT_DATA_ALT				X			X	X											
T.CONFIDENTIAL_DATA_DIS					X		X	X											
T.CONFIDENTIAL_DATA_ALT						X	X	X											
P.AUTHORIZATION							X	X											
P.VALIDATION									X										
P.AUDIT										X	X	X							
P.FAX													X						
P.ENCRYPTION																X			
A.PHYSICAL_PROTECTION														X					
A.NETWORK_PROTECTION															X				
A.ADMIN																	X		
A.TRUSTED_ADMIN																		X	
A.USER																			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.DOCUMENT_DATA_DIS

T.DOCUMENT_DATA_DIS is countered by O.DOCUMENT_DATA_DIS, O.AUTHORIZATION, and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.DOCUMENT_DATA_DIS, the TOE protects document data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the document data.

T.DOCUMENT_DATA_DIS is countered by these objectives.

T.DOCUMENT_DATA_ALT

T.DOCUMENT_DATA_ALT is countered by O.DOCUMENT_DATA_ALT, O.AUTHORIZATION, and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.DOCUMENT_DATA_ALT, the TOE protects document data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the document data.

T.DOCUMENT_DATA_ALT is countered by these objectives.

T.JOB_ALT

T.JOB_ALT is countered by O.JOB_ALT, O.AUTHORIZATION, and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.JOB_ALT, the TOE protects the user job data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the user job data.

T.JOB_ALT is countered by these objectives.

T.PROTECT_DATA_ALT

T.PROTECT_DATA_ALT is countered by O.PROTECT_DATA_ALT, O.AUTHORIZATION, and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.PROTECT_DATA_ALT, the TOE protects the TSF protected data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF protected data.

T.PROTECT_DATA_ALT is countered by these objectives.

T.CONFIDENTIAL_DATA_DIS

T.CONFIDENTIAL_DATA_DIS is countered by O.CONFIDENTIAL_DATA_DIS, O.AUTHORIZATION, and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.CONFIDENTIAL_DATA_DIS, the TOE protects the TSF confidential data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

T.CONFIDENTIAL_DATA_DIS is countered by these objectives.

T.CONFIDENTIAL_DATA_ALT

T.CONFIDENTIAL_DATA_ALT is countered by O.CONFIDENTIAL_DATA_ALT, O.AUTHORIZATION, and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE. By O.CONFIDENTIAL_DATA_ALT, the TOE protects the TSF confidential data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data.

T.CONFIDENTIAL_DATA_ALT is countered by these objectives.

P.AUTHORIZATION

P.AUTHORIZATION is countered by O.AUTHORIZATION and OE.AUTHORIZED_USER.

By OE.AUTHORIZED_USER, the MFP administrator gives the authority to use the TOE to users in accordance with the security policies and procedures of their organisation. By O.AUTHORIZATION, the TOE requires identification and authentication of users, and users are authorised in accordance with the security policies before being allowed to use the TOE.

P.AUTHORIZATION is enforced by these objectives.

P.VALIDATION

P.VALIDATION is countered by O.VALIDATION.

By O.VALIDATION, the TOE provides measures for self-verifying the executable code of the TSF.

P.VALIDATION is enforced by this objective.

P.AUDIT

P.AUDIT is countered by O.AUDIT, OE.AUDIT, OE.AUDIT_MANAGE.

By O.AUDIT, the TOE creates and maintains logs of TOE security-relevant events as audit log and protects them from disclosure or alteration by unauthorised persons. It also provides audit logs in a format that can be verified by unauthorised persons.

On the other hand, by OE.AUDIT, the MFP administrator ensures that audit logs that are exported to a trusted IT product are protected from being accessed and altered by unauthorised persons. In addition, by OE.AUDIT_MANAGE, the MFP administrator reviews audit logs at appropriate intervals for detecting security violations or unusual patterns of activity.

P.AUDIT is enforced by these objectives.

P.FAX

P.FAX is countered by O.FAX.

By O.FAX, for provision of the Fax Function over the telephone line by the TOE, the TOE ensures the separation between the telephone line and the LAN.

P.FAX is enforced by this objective.

P.ENCRYPTION

P.ENCRYPTION is countered by O.EMMC_ENCRYPTION.

By O.EMMC_ENCRYPTION, the TOE provides the function to encrypt data first and then store it in the eMMC.

P.ENCRYPTION is enforced by this objective.

A.PHYSICAL_PROTECTION

A.PHYSICAL_PROTECTION is operated under OE.PHYSICAL_PROTECTION.

By OE.PHYSICAL_PROTECTION, the TOE is installed in a secure and monitored area in accordance with the guidance documents and a chance of physical access by unspecified number of persons is restricted.

A.PHYSICAL_PROTECTION is fulfilled by this objective.

A.NETWORK_PROTECTION

A.NETWORK_PROTECTION is operated under OE.NETWORK_PROTECTION.

By OE.NETWORK_PROTECTION, the MFP administrator ensures that the TOE is installed in an operational environment protected from any external attempt to directly access the TOE's LAN interfaces.

A.NETWORK_PROTECTION is fulfilled by this objective.

A.ADMIN

A.ADMIN is operated under OE.TRAINED_ADMIN.

By OE.TRAINED_ADMIN, the responsible manager of MFP ensures that MFP administrators are trained to correctly configure and operate the TOE in accordance with the guidance documents following the security policies and procedures of their organisation and they have the competence to follow those policies and procedures.

A.ADMIN is fulfilled by this objective.

A.TRUSTED_ADMIN

A.TRUSTED_ADMIN is operated under OE.TRUSTED_ADMIN.

By OE.TRUSTED_ADMIN, the responsible manager of MFP appoints administrators who will not use their privileged access rights for malicious purposes according to the guidance documents.

A.TRUSTED_ADMIN is fulfilled by this objective.

A.USER

A.USER is operated under OE.TRAINED_USER.

By OE.TRAINED_USER, the MFP administrator instructs the users in accordance with the guidance documents to make them aware of the security policies and procedures of their organisation, and the users follow those policies and procedures.

A.USER is fulfilled by this objective.

5 Extended Components Definition

This section describes Extended Components Definition.

5.1 Fax separation (FDP_FXS_EXP)

Family behaviour

This family addresses the requirements for the separation between the fax telephone line and the LAN to which the TOE is connected.

Component levelling

FDP_FXS_EXP.1 Fax separation requires that the fax interface is not available to create a network bridge between the telephone line and the LAN to which the TOE is connected.

Management: **FDP_FXS_EXP.1**

- There are no management actions foreseen.

Audit: **FDP_FXS_EXP.1**

There are no auditable events foreseen.

FDP_FXS_EXP.1 Fax separation

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_FXS_EXP.1.1 **The TSF shall prohibit communication via a fax interface, except for transmission or reception of user data using a fax protocol.**

Rationale:

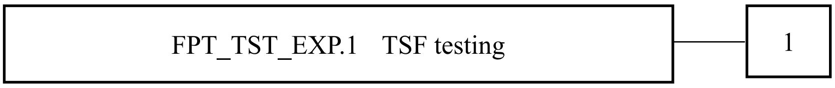
The fax separation protects the LAN against attacks from the telephone lines. Common Criteria does not provide suitable SFRs for protecting TSF or user data. Since this extended component protects TSF data or user data, it is considered as a component of the FDP class.

5.2 TSF testing (FPT_TST_EXP)

Family behaviour

This family addresses TSF's self-testing requirements for verifying the integrity of executable code in the TSF.

Component levelling



FPT_TST_EXP.1 TSF testing requires a suite of self-tests that runs at initial startup to verify the integrity of executable code in the TSF.

Management: FPT_TST_EXP.1

- There are no management actions foreseen.

Audit: FPT_TST_EXP.1

There are no auditable events foreseen.

FPT_TST_EXP.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST_EXP.1.1 **The TSF shall run a suite of self-tests at initial startup (and power-on) to verify the integrity of executable code in the TSF.**

Rationale:

The TSF testing ensures that the integrity of executable code in the TSF is verified. The target of integrity verification is different from that of the SFRs provided by Common Criteria. Since this extended component protects the TOE, it is considered as a component of the FPT class.

6 Security Requirements

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

The terms used in this section are defined in Table 11.

Table 11: Terms 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	Information contained in the user's document in electronic or hard-copy format. Document data stored and saved in the eMMC (stored document data) and document data received from the printer driver and temporarily saved in the TOE (temporarily-saved document) are included. Stored document data includes scanned documents, fax transmission documents, fax reception documents, stored print documents, and Document Server documents.
	Temporarily-saved document	Document data received from the printer driver and temporarily saved in the TOE.
	Scanned document	One of the stored document data types. Document data stored in the TOE by the Scanner Function.
	Fax transmission document	One of the stored document data types. Document data received from the fax driver and stored in the TOE, and document data stored in the TOE for sending by the Fax Function.
	Fax reception document	One of the stored document data types. Document data stored in the TOE by means of fax reception from an external fax via a telephone line instructed by the TOE.

Classification of Term	Name of Term	Description of Term
	Stored print document	One of the stored document data types. Document data received from the printer driver and stored in the TOE with stored print specified as the print method.
	Document Server document	One of the stored document data types. Document data stored in the TOE by using the Copy or Document Server Function, or document data received from the printer driver and stored in the TOE with Document Server storage specified as the print method.
	User job data	Information related to the user's document or document processing job. Information regarding a sequence of operations of each TOE function (Copy Function, Scanner Function, Printer Function, Fax Transmission Function, Fax Reception Function, and Document Server Function) from beginning to end.
Operation	Read	To perform print, fax transmission, e-mail transmission of attachments, folder transmission, download, or preview.
	Delete	To delete TSF data or objects.
	Newly create	To newly create TSF data.
	Query	To refer to TSF data.
	Modify	To modify TSF data or objects.
	Change_default	To change the default value of TSF data.
Security attribute	Login user name	User identifier associated with any of the normal user, MFP administrator, and supervisor. The TOE identifies users by this identifier.
	User privilege	Any role of normal user, MFP administrator, or supervisor who uses the TOE, and the privilege according to that role.

Classification of Term	Name of Term	Description of Term
	Document data owner information	The security attribute of document data (temporarily-saved document data, scanned documents, fax transmission documents, stored print documents, and Document Server documents). The owner information (the login user name) of document data (except fax reception documents) is set.
	List of users who have been granted access permission for the document data	The security attribute of document data (temporarily-saved document data, scanned documents, fax transmission documents, stored print documents, and Document Server documents). The information of users (the login user names) who are allowed access (viewing) document data (except fax reception documents) is set. The document data owner can allow other normal users to read the document data.
	Fax reception document user	The security attribute of fax reception documents. The list of the login user names of users who have been granted access (read and delete) permission for fax reception documents is set. The users are managed with one list for all fax reception documents.
	User job data owner information	The security attribute of user job data. The information of user job data owners (the login user name) is set.
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 operate the MFP application (that is, run and cancel the Copy Function, Fax Function, Scanner Function, Printer Function, and Document Server Function).

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 documents - Unlocking locked-out normal users and supervisor
	Supervisor	A user who has the privilege to manage the TOE, including: - Changing login password of MFP administrators - Unlocking locked-out MFP administrators

6.1 Security Functional Requirements

This section describes the TOE security functional requirements for fulfilling the security objectives defined in section 4.1.

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, choose one of: *minimum, basic, detailed, not specified*] level of audit; and

c) [assignment: *other specifically defined auditable events*].

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

- ***not specified***

[assignment: *other specifically defined auditable events*]

- ***Auditable events of the TOE shown in Table 12***

FAU_GEN.1.2 **The TSF shall record within each audit record at least the following information:**
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

[assignment: *other audit relevant information*]

- ***All login user names that attempted the user identification for FIA_UID.1, job type, communicating devices with the trusted channel, lockout operation type, locked out user, and locked out user who is to be released***

The related SFRs and auditable events for the TOE are listed in Table 12.

Table 12: 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 printing temporarily-saved document data, fax transmission documents, fax reception documents, stored print documents, and Document Server documents - Start and end of downloading scanned documents, fax transmission documents, and fax reception documents - Start and end of sending scanned documents by e-mail transmission of attachments - Start and end of sending scanned documents by folder transmission - Start and end of sending fax transmission documents by fax transmission - Deletion of temporarily-saved document data, scanned documents, fax transmission documents, fax reception documents, stored print documents, and Document Server documents - Deletion of user job data	FDP_ACF.1
Starting and releasing lockout	FIA_AFL.1
Success and failure of login operation	FIA_UAU.1 FIA_UID.1
Use of the management functions in Table 24	FMT_SMF.1 FPT_STM.1
Termination of session by auto logout	FTA_SSL.3

Auditable Event	Related SFR
Failure of the trusted channel functions	FTP_ITC.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, choose one of: *prevent, detect*] unauthorized modifications to the stored audit records in the audit trail.**

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

- ***prevent***

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, choose one of: *"ignore audited events", "prevent audited events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*]** and [assignment: ***other*** *actions to be taken in case of audit storage failure*] if the audit trail is **full**.

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

- ***"overwrite the oldest stored audit records"***

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

- *None*

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: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.**

[assignment: *authorised users*]

- ***MFP administrator***

[assignment: *the list of audit information*]

- ***All audit logs***

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: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].**

[assignment: *list of standards*]

- ***None***

[assignment: *cryptographic key generation algorithm*]

- ***Random number generation using AES-128***

[assignment: *cryptographic key sizes*]

- ***256 bits***

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: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].**

[assignment: *list of standards*]

- ***None***

[assignment: *cryptographic key destruction method*]

- ***Overwrite with 0***

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: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].**

[assignment: *list of standards*]

- ***FIPS197***

[assignment: *cryptographic algorithm*]

- ***AES***

[assignment: *cryptographic key sizes*]

- ***256 bits***

[assignment: *list of cryptographic operations*]

- ***Encryption of data to be written to the eMMC***
  Decryption of data to be read from the eMMC

6.1.3 Class FDP: User data protection

6.1.3.1. FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 **The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].**

[assignment: *list of subjects, objects, and operations among subjects and objects covered in the SFP*]

- ***List of subjects, objects, and operations among subjects and objects shown in Table 13***

[assignment: *access control SFP*]

- ***User data access control SFP***

Table 13: List of Subjects, Objects, and Operations among Subjects and Objects

Subjects	Objects	Operations
Normal user process MFP administrator process Supervisor process	Temporarily-saved document data Scanned document Fax transmission document Fax reception document Stored print document Document Server document	Read Delete Modify
	User job data	Delete Modify

6.1.3.2. FDP_ACF.1 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 **The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or a named group of SFP-relevant security attributes*].**

[assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or a named group of SFP- relevant security attributes*]

- ***Subjects, objects, and for each, the security attributes shown in Table 14***

[assignment: *access control SFP*]

- ***User data access control SFP***

Table 14: Subjects, Objects, and Security Attributes

Category	Subjects or Objects	Security Attributes
Subject	Normal user process	Login user name User privilege
Subject	MFP administrator process	Login user name User privilege
Subject	Supervisor process	Login user name User privilege
Object	Temporarily-saved document data	Document data owner information
Object	Scanned document Fax transmission document Stored print document Document Server document	Document data owner information List of users who have been granted access permission for the document data
Object	Fax reception document	Fax reception document user
Object	User job data	User job data owner information

FDP_ACF.1.2 **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].**

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

- ***Rules to control operations among subjects and objects shown in Table 15***

Table 15: Rules to Control Operations among Subjects and Objects

Objects	Operations	Subjects (Security Attributes)	Rules of User Data Access Control SFP
Temporarily-saved document	Read Delete	Normal user process (Login user name, user privilege)	Not allowed. However, operation is allowed when the login user name of the normal user process and the login user name registered in the "document data owner information" of the object match.

Objects	Operations	Subjects (Security Attributes)	Rules of User Data Access Control SFP
Scanned document Fax transmission document Stored print document Document Server document	Read	Normal user process (Login user name, user privilege)	Not allowed. However, operation is allowed when the login user name of the normal user process and the login user name registered in the "Document data owner information" of the object match. Further, operation is allowed when the login user name of the normal user process and the login user name registered in the "list of users who have been granted access permission for the document data" of the object match.
Scanned document Fax transmission document Stored print document Document Server document	Delete	Normal user process (Login user name, user privilege)	Not allowed. However, operation is allowed when the login user name of the normal user process and the login user name registered in the "document data owner information" of the object match.
Fax transmission document	Read Delete	Normal user process (Login user name, user privilege)	Not allowed. However, operation is allowed when the login user name of the normal user process and the login user name registered in the "fax reception document user " of the object match.
User job data	Delete	Normal user process (Login user name, user privilege)	Not allowed. (*1) However, operation is allowed when the login user name of the normal user process and the login user name registered in the "user job data owner information " of the object match.

(*1) No interface is provided.

FDP_ACF.1.3 **The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].**

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

- ***Rules that explicitly authorise access shown in Table 16***

Table 16: Rules That Explicitly Authorise Access

Objects	Operations	Subjects (Security Attributes)	Rules of User Data Access Control SFP
Temporarily-saved document Scanned document Fax transmission document Stored print document Document Server document	Delete	MFP administrator process (User privilege, login user name)	Allowed.
Scanned document Fax transmission document Document Server document	Read	MFP administrator process (User privilege, login user name)	Allowed.
User job data	Delete	MFP administrator process (User privilege, login user name)	Allowed.

FDP_ACF.1.4 **The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].**

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

- ***Rules that explicitly deny access shown in Table 17***

Table 17: Rules That Explicitly Deny Access

Objects	Operations	Subjects (Security Attributes)	Rules of User Data Access Control SFP
Temporarily-saved document Stored print document	Read	MFP administrator process (User privilege, login user name)	Denied. (*1)
Fax transmission document	Read Delete	MFP administrator process (User privilege, login user name)	Denied. (*1)

Objects	Operations	Subjects (Security Attributes)	Rules of User Data Access Control SFP
Temporarily-saved document Scanned document Fax transmission document Fax reception document Stored print document Document Server document	Read Delete	Supervisor process (User privilege, login user name)	Denied. (*1)
Temporarily-saved document Scanned document Fax transmission document Fax reception document Stored print document Document Server document	Modify	Normal user process (User privilege, login user name)	For any subject, document data operation is denied. (*1)
		MFP administrator process (User privilege, login user name)	
		Supervisor process (User privilege, login user name)	
User job data	Delete	Supervisor process (User privilege, login user name)	Denied. (*1)
User job data	Modify	Normal user process (User privilege, login user name)	For any subject, user job data operation is denied. (*1)
		MFP administrator process (User privilege, login user name)	
		Supervisor process (User privilege, login user name)	

(*1) No interface is provided.

6.1.3.3. FDP_FXS_EXP.1 Fax separation

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_FXS_EXP.1.1 **The TSF shall prohibit communication via a fax interface, except for transmission or reception of user data using a fax protocol.**

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: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: list of authentication events].**

[assignment: ***list of authentication events*****]**

- ***Authentication events shown in Table 18***

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

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

[assignment: range of acceptable values]

- ***1 to 5***

Table 18: List of Authentication Events

Authentication Events
User authentication using the Operation Panel
User authentication using 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:** ***list of actions*****].**

[selection: ***met, surpassed*****]**

- ***met, surpassed***

[assignment: ***the list of actions*****]**

- ***Actions shown in Table 19***

Table 19: List of Actions for Authentication Failure

Unsuccessfully Authenticated Users	Actions 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: *list of security attributes*]**

[assignment: *list of security attributes*]

- ***Login user name, user privilege***

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: a *defined quality metric*].**

[assignment: a *defined quality metric*]

- ***Quality metrics are as follows:***

(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 (8-32 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 supervisors***

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: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.**

[assignment: *list of TSF mediated actions*]

- ***Viewing of the list of user job data, WIM Help, system status, counter and information of inquiries, and execution of fax reception***

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: *list of feedback*] to the user while the authentication is in progress.**

[assignment: *list of feedback*]

- ***Dummy letters***

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: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.**

[assignment: *list of TSF-mediated actions*]

- ***Viewing of the list of user job data, WIM Help, system status, counter and information of inquiries, and execution of fax reception***

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

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: *list of user security attributes*]**

[assignment: *list of user security attributes*]

- ***Login user name, user privilege***

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

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

- ***None***

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

[assignment: *rules for changing of attributes*]

- ***None***

6.1.5 Class FMT: Security management

6.1.5.1. FMT_MOF.1 Control of the behaviour of the Security Functions

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Function

FMT_MOF.1.1 **The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: the *authorised and identified roles*].**

[assignment: *list of functions*]

- ***syslog transfer function***

[selection: *determine the behaviour of, disable, enable, modify the behaviour of]*

- ***disable, enable***

[assignment: *the authorised and identified roles*]

- ***MFP administrator***

6.1.5.2. FMT_MSA.1 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 Function

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

[assignment: *list of security attributes*]

- ***Security attributes in Table 20***

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

- ***change_default, delete, [assignment: other operations]***

[assignment: other operations]

- ***Newly create, modify***

[assignment: the *authorised and identified roles*]

- ***Roles (user privileges) for which the operations i*n *Table 20 are allowed***

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

- ***User data access control SFP(s)***

Table 20: User Privilege by Security Attribute

Security Attributes	Operations	Roles (User Privileges) for Which Operations are Allowed
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 privilege	Modify	No role with the operation permission
Document data owner information	Modify	No role with the operation permission
List of users who have been granted access permission for the document data	Modify	MFP administrator Document data owner (normal user)
	Change_default	MFP administrator

Security Attributes	Operations	Roles (User Privileges) for Which Operations are Allowed
Fax reception document user	Modify	MFP administrator
User job data owner information	Modify	No role with the operation permission

6.1.5.3. FMT_MSA.3 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 **The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.**

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

- ***restrictive***

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

- ***User data access control SFP***

FMT_MSA.3.2 **The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.**

[assignment: the *authorised identified roles*]

- ***Roles (user privileges) for which the operation in Table 21 is allowed***

Table 21: Roles for Which Operation to Overwrite Default Values is Allowed

Objects	Security Attributes	Roles (User Privileges) for Which the Operation is Allowed
Temporarily-saved document Scanned document Fax transmission document Stored print document Document Server document	Document data owner information	No role with the operation permission
Scanned document	List of users who have been granted access permission for the document data	Normal user in question who creates the document data

Objects	Security Attributes	Roles (User Privileges) for Which the Operation is Allowed
Fax transmission document	List of users who have been granted access permission for the document data	Normal user in question who creates the document data (Overwriting the default values is allowed only when the document data is stored from the Operation Panel. There is no interface for overwriting default values when the document data is stored from the fax driver.)
Fax reception document	Fax reception document user	No role with the operation permission
Stored print document	List of users who have been granted access permission for the document data	No role with the operation permission
Document Server document	List of users who have been granted access permission for the document data	Normal user in question who creates the document data (Overwriting the default values is allowed only when the document data is stored from the Operation Panel. There is no interface for overwriting default values when the document data is stored from the printer driver.)
User job data	User job data owner information	No role with the operation permission

6.1.5.4. 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 Function

FMT_MTD.1.1(a) **The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].**

[assignment: *list of TSF data*]

- ***TSF data in Table 22***

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

- ***query, delete, [assignment: other operations]***

[assignment: other operations]

- ***Newly create, modify***

[assignment: *the authorised identified roles*]

- ***Roles (user privileges) for which the operations in Table 22 are allowed***

Table 22: List of TSF Data

Category	TSF data	Operations	Roles (User Privileges) for Which Operations are Allowed
TSF protected data	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
	Destination folder	Newly create Modify Delete	MFP administrator
	Audit log settings	Modify	MFP administrator
	Cryptographic communication settings	Modify	MFP administrator
TSF confidential data	Login password [When associated with a normal user]	Modify	Normal user in question MFP administrator
		Newly create	MFP administrator
	Login password [When associated with an MFP administrator]	Modify	MFP administrator in question Supervisor
		Newly create	MFP administrator
	Login password [When associated with a supervisor]	Modify	Supervisor
	eMMC cryptographic key	Newly create Query Delete	MFP administrator

6.1.5.5. 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 Function

FMT_MTD.1.1(b) **The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*] the [assignment: *list of TSF data*] to [assignment: the *authorised identified roles*].**

[assignment: *list of TSF data*]

- ***TSF data in Table 23***

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

- ***Query***

[assignment: the *authorised identified roles*]

- ***Roles (user privileges) for which the operation in Table 23 is allowed***

Table 23: List of TSF Data

Category	TSF data	Operations	Roles (User Privileges) for Which Operations are Allowed
TSF confidential data	Login password	Query	No roles for which operations are allowed

6.1.5.6. FMT_SMF.1 Specification of Management Function

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

- ***Management functions listed in Table 24***

Table 24: List of Specification of Management Functions

Management Functions
Disable and enable the syslog transfer function
Newly create, modify, and delete login user names
Modify the list of users who have been granted access permission for the document data, and change the default value of it
Modify fax reception document users
Newly create and modify login passwords
Query, delete, and newly create eMMC cryptographic keys
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

6.1.5.7. 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: the *authorised identified roles*].**

[assignment: *the authorised identified roles*]

- ***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_EXP.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST_EXP.1.1 **The TSF shall run a suite of self-tests at initial startup (and power-on) to verify the integrity of executable code in the TSF.**

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 an interactive session after [assignment: *time interval of user inactivity*]**

[assignment: *time interval of user inactivity*]

- ***Time specified by the MFP administrator***

6.1.8 Class FTP: Trusted paths/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.**

[selection: *the TSF, another trusted IT product*]

- ***The TSF, another trusted IT product***

FTP_ITC.1.3 **The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].**

[assignment: *list of functions for which a trusted channel is required*]

- ***Scanner function***
- ***syslog transfer function***

- ***Fax Function***
- ***Printer Function***
- ***WIM Function***

6.2 Security Assurance Requirements

The evaluation assurance level of this TOE is EAL2. Table 25 lists the assurance components of the TOE.

Table 25: TOE Security Assurance Requirements (EAL2)

Assurance Classes	Assurance Components	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
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 defined in "4 Security Objectives" are fulfilled.

6.3.1 Tracing

Table 26 describes the relationship between the TOE security functional requirements and TOE security objectives. Items in **bold** provide the primal (**P**) fulfillment of the objectives, and items in standard typeface support (S) its fulfillment. Table 26 describes that each TOE security functional requirement fulfils at least one TOE security objective.

Table 26: Correspondence between Security Objectives and Functional Requirements

	O.DOCUMENT_DATA_DIS	O.DOCUMENT_DATA_ALT	O.JOB_ALT	O.PROTECT_DATA_ALT	O.CONFIDENTIAL_DATA_DIS	O.CONFIDENTIAL_DATA_ALT	O.AUTHORIZATION	O.FAX	O.VALIDATION	O.AUDIT	O.EMMC_ENCRYPTION
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	**P**	**P**	**P**								
FDP_ACF.1	**P**	**P**	**P**								
FDP_FXS_EXP.1								**P**			
FIA_AFL.1							S				
FIA_ATD.1							S				
FIA_SOS.1							S				
FIA_UAU.1							**P**				
FIA_UAU.7							S				
FIA_UID.1	S	S	S	S	S	S	**P**			S	
FIA_USB.1							**P**				
FMT_MOF.1				**P**							
FMT_MSA.1	S	S	S	**P**							

	O.DOCUMENT_DATA_DIS	O.DOCUMENT_DATA_ALT	O.JOB_ALT	O.PROTECT_DATA_ALT	O.CONFIDENTIAL_DATA_DIS	O.CONFIDENTIAL_DATA_ALT	O.AUTHORIZATION	O.FAX	O.VALIDATION	O.AUDIT	O.EMMC_ENCRYPTION
FMT_MSA.3	S	S	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_EXP.1									**P**		
FTA_SSL.3							S				
FTP_ITC.1	**P**	**P**	**P**	**P**	**P**	**P**					

6.3.2 Justification of Traceability

This section describes how the TOE security objectives are fulfilled by the TOE security functional requirements corresponding to the TOE security objectives.

O.DOCUMENT_DATA_DIS Protection of document data disclosure

O.DOCUMENT_DATA_DIS is the security objective where the TOE protects the document data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the document data. To fulfil this security objective, it is required to implement the following SFRs.

(1) FDP_ACC.1, FDP_ACF.1

FDP_ACC.1 and FDP_ACF.1 ensure that an access control policy for document data is defined and access control functions are provided in accordance with the access control policy.

FDP_ACC.1 and FDP_ACF.1 are major SFRs to fulfill O.DOCUMENT_DATA_DIS.

(2) FTP_ITC.1

FTP_ITC.1 ensures that document data sent and received by the TOE via the LAN is protected.

FTP_ITC.1 is a major SFR to fulfill O.DOCUMENT_DATA_DIS.

(3) FMT_MSA.1

FMT_MSA.1 ensures that the management of security attributes is restricted to specific users.

FMT_MSA.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_DIS.

(4) FMT_MSA.3

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

FMT_MSA.3 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_DIS.

(5) FMT_SMF.1

FMT_SMF.1 ensures that the necessary management functions for the security functions are implemented.

FMT_SMF.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_DIS.

(6) FMT_SMR.1

FMT_SMR.1 ensures that the authorised user roles are maintained.

FMT_SMR.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_DIS.

(7) FIA_UID.1

FIA_UID.1 ensures that persons who attempt to use the TOE from the Operation Panel or the client computer on the network are identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_DIS.

O.DOCUMENT_DATA_DIS can be fulfilled by implementing these security functional requirements.

O.DOCUMENT_DATA_ALT Protection of document data alteration

O.DOCUMENT_DATA_ALT is the security objective where the TOE protects the document data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the document data. To fulfil this security objective, it is required to implement the following SFRs.

(1) FDP_ACC.1, FDP_ACF.1

FDP_ACC.1 and FDP_ACF.1 ensure that an access control policy for document data is defined and access control functions are provided in accordance with the access control policy.

FDP_ACC.1 and FDP_ACF.1 are major SFRs to fulfill O.DOCUMENT_DATA_ALT.

(2) FTP_ITC.1

FTP_ITC.1 ensures that document data sent and received by the TOE via the LAN is protected.

FTP_ITC.1 is a major SFR to fulfill O.DOCUMENT_DATA_ALT.

(3) FMT_MSA.1

FMT_MSA.1 ensures that the management of security attributes is restricted to specific users.

FMT_MSA.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_ALT.

(4) FMT_MSA.3

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

FMT_MSA.3 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_ALT.

(5) FMT_SMF.1

FMT_SMF.1 ensures that the necessary management functions for the security functions are implemented.

FMT_SMF.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_ALT.

(6) FMT_SMR.1

FMT_SMR.1 ensures that the authorised user roles are maintained.

FMT_SMR.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_ALT.

(7) FIA_UID.1

FIA_UID.1 ensures that persons who attempt to use the TOE from the Operation Panel or the client computer on the network are identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.DOCUMENT_DATA_ALT.

O.DOCUMENT_DATA_ALT can be fulfilled by implementing these security functional requirements.

O.JOB_ALT Protection of user job data alteration

O.JOB_ALT is the security objective where the TOE protects the user job data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the user job data. To fulfil this security objective, it is required to implement the following SFRs.

(1) FDP_ACC.1, FDP_ACF.1

FDP_ACC.1 and FDP_ACF.1 ensure that an access control policy for user job data is defined and access control functions are provided in accordance with the access control policy.

FDP_ACC.1 and FDP_ACF.1 are major SFRs to fulfill O.JOB_ALT.

(2) FTP_ITC.1

FTP_ITC.1 ensures that user job data sent and received by the TOE via the LAN is protected.

FTP_ITC.1 is a major SFR to fulfill O.JOB_ALT.

(3) FMT_MSA.1

FMT_MSA.1 ensures that the management of security attributes is restricted to specific users.

FMT_MSA.1 is an SFR that supports the fulfillment of O.JOB_ALT.

(4) FMT_MSA.3

FMT_MSA.3 manages the default security attributes when user job data is generated.

FMT_MSA.3 is an SFR that supports the fulfillment of O.JOB_ALT.

(5) FMT_SMF.1

FMT_SMF.1 ensures that the necessary management functions for the security functions are implemented.

FMT_SMF.1 is an SFR that supports the fulfillment of O.JOB_ALT.

(6) FMT_SMR.1

FMT_SMR.1 ensures that the authorised user roles are maintained.

FMT_SMR.1 is an SFR that supports the fulfillment of O.JOB_ALT.

(7) FIA_UID.1

FIA_UID.1 ensures that persons who attempt to use the TOE from the Operation Panel or the client computer on the network are identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.JOB_ALT.

O.JOB_ALT can be fulfilled by implementing these security functional requirements.

O.PROTECT_DATA_ALT Protection of TSF protected data alteration

O.PROTECT_DATA_ALT is the security objective where the TOE protects the TSF protected data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF protected data. To fulfil this security objective, it is required to implement the following SFRs.

(1) FMT_MTD.1(a)

FMT_MTD.1(a) ensures that the operation of TSF protected data is restricted to authorised users.

FMT_MTD.1(a) is a major SFR to fulfill O.PROTECT_DATA_ALT.

(2) FMT_SMF.1

FMT_SMF.1 ensures that the necessary management functions for the security functions are implemented.

FMT_SMF.1 is an SFR that supports the fulfillment of O.PROTECT_DATA_ALT.

(3) FMT_SMR.1

FMT_SMR.1 ensures that the authorised user roles are maintained.

FMT_SMR.1 is an SFR that supports the fulfillment of O.PROTECT_DATA_ALT.

(4) FTP_ITC.1

FTP_ITC.1 ensures that TSF protected data sent and received by the TOE via the LAN is protected.

FTP_ITC.1 is a major SFR to fulfill O.PROTECT_DATA_ALT.

(5) FMT_MOF.1

FMT_MOF.1 ensures that only MFP administrators are allowed to manage security functions.

FMT_MOF.1 is a major SFR to fulfill O.PROTECT_DATA_ALT.

(6) FMT_MSA.1

FMT_MSA.1 ensures that the management of security attributes is restricted to specific users.

FMT_MSA.1 is a major SFR to fulfill O.PROTECT_DATA_ALT.

(7) FIA_UID.1

FIA_UID.1 ensures that persons who attempt to use the TOE from the Operation Panel or the client computer on the network are identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.PROTECT_DATA_ALT.

O.PROTECT_DATA_ALT can be fulfilled by implementing these security functional requirements.

O.CONFIDENTIAL_DATA_DIS Protection of TSF confidential data disclosure

O.CONFIDENTIAL_DATA_DIS is the security objective where the TOE protects the TSF confidential data from unauthorised disclosure by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data. To fulfil this security objective, it is required to implement the following SFRs.

(1) FMT_MTD.1(a), FMT_MTD.1(b)

FMT_MTD.1(a) and FMT_MTD.1(b) ensure that the operation of TSF confidential data is restricted to authorised users.

FMT_MTD.1(a) and FMT_MTD.1(b) are major SFRs to fulfill O.CONFIDENTIAL_DATA_DIS.

(2) FMT_SMF.1

FMT_SMF.1 ensures that the necessary management functions for the security functions are implemented.

FMT_SMF.1 is an SFR that supports the fulfillment of O.CONFIDENTIAL_DATA_DIS.

(3) FMT_SMR.1
FMT_SMR.1 ensures that the authorised user roles are maintained.

FMT_SMR.1 is an SFR that supports the fulfillment of O.CONFIDENTIAL_DATA_DIS.

(4) FTP_ITC.1
FTP_ITC.1 ensures that TSF confidential data sent and received by the TOE via the LAN is protected.

FTP_ITC.1 is a major SFR to fulfill O.CONFIDENTIAL_DATA_DIS.

(5) FIA_UID.1
FIA_UID.1 ensures that persons who attempt to use the TOE from the Operation Panel or the client computer on the network are identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.CONFIDENTIAL_DATA_DIS.

(6) FAU_SAR.1, FAU_SAR.2
FAU_SAR.1 ensures that audit logs can be read in a format that can be verified by the MFP administrator. FAU_SAR.2 ensures that anyone other than the MFP administrator is prohibited to read audit logs.

FAU_SAR.1 and FAU_SAR.2 are major SFRs to fulfill O.CONFIDENTIAL_DATA_DIS.

O.CONFIDENTIAL_DATA_DIS can be fulfilled by implementing these security functional requirements.

O.CONFIDENTIAL_DATA_ALT Protection of TSF confidential data alteration

O.CONFIDENTIAL_DATA_ALT is the security objective where the TOE protects the TSF confidential data from unauthorised alteration by persons without a login user name, or by persons with a login user name but without an access permission to the TSF confidential data. To fulfil this security objective, it is required to implement the following SFRs.

(1) FMT_MTD.1(a)
FMT_MTD.1(a) ensures that the operation of TSF confidential data is restricted to authorised users.

FMT_MTD.1(a) is a major SFR to fulfill O.CONFIDENTIAL_DATA_ALT.

(2) FMT_SMF.1
FMT_SMF.1 ensures that the necessary management functions for the security functions are implemented.

FMT_SMF.1 is an SFR that supports the fulfillment of O.CONFIDENTIAL_DATA_ALT.

(3) FMT_SMR.1
FMT_SMR.1 ensures that the authorised user roles are maintained.

FMT_SMR.1 is an SFR that supports the fulfillment of O.CONFIDENTIAL_DATA_ALT.

(4) FTP_ITC.1
FTP_ITC.1 ensures that TSF confidential data sent and received by the TOE via the LAN is protected.

FTP_ITC.1 is a major SFR to fulfill O.CONFIDENTIAL_DATA_ALT.

(5) FIA_UID.1
FIA_UID.1 ensures that persons who attempt to use the TOE from the Operation Panel or the client computer on the network are identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.CONFIDENTIAL_DATA_ALT.

(6) FAU_STG.1
FAU_STG.1 ensures that audit logs are protected from alteration.

FAU_STG.1 is a major SFR to fulfill O.CONFIDENTIAL_DATA_ALT.

O.CONFIDENTIAL_DATA_ALT can be fulfilled by implementing these security functional requirements.

O.AUTHORIZATION User identification and authentication

O.AUTHORIZATION is the security objective where it is ensured that the TOE requires identification and authentication of users and users are authorised in accordance with the security policies before being allowed to use the TOE. To fulfil this security objective, it is required to implement the following SFRs.

(1) FIA_UID.1, FIA_UAU.1

FIA_UID.1 and FIA_UAU.1 ensure that persons who attempt to use the TOE from the Operation Panel or the client computer on the network are identified and authenticated.

FIA_UID.1 and FIA_UAU.1 are major SFRs to fulfill O.AUTHORIZATION.

(2) FIA_USB.1

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

FIA_USB.1 is a major SFR to fulfill O.AUTHORIZATION.

(3) FIA_ATD.1

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

FIA_ATD.1 is an SFR that supports the fulfillment of O.AUTHORIZATION.

(4) FIA_UAU.7

FIA_UAU.7 ensures that the disclosure of login passwords is prevented by displaying dummy letters as authentication feedback.

FIA_UAU.7 is an SFR that supports the fulfillment of O.AUTHORIZATION.

(5) 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.

FIA_SOS.1 is an SFR that supports the fulfillment of O.AUTHORIZATION.

(6) FIA_AFL.1

FIA_AFL.1 ensures that users who have repeatedly failed authentication a certain number of times are not allowed to access the TOE for a certain period of time.

FIA_AFL.1 is an SFR that supports the fulfillment of O.AUTHORIZATION.

(7) 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 and the logged-in state is cancelled. Therefore, the user's session is managed and the inactive session is terminated.

FTA_SSL.3 is an SFR that supports the fulfillment of O.AUTHORIZATION.

O.AUTHORIZATION can be fulfilled by implementing these security functional requirements.

O.FAX Management of external interfaces by TOE

O.FAX is the security objective to ensure that, for provision of the Fax Function over the telephone line by the TOE, the TOE ensures the separation between the telephone line and the LAN. To fulfil this security objective, it is required to implement the following SFRs.

(1) FDP_FXS_EXP.1

FDP_FXS_EXP.1 ensures that communication via a fax interface is prohibited, except for transmission or reception of user data using a fax protocol.

FDP_FXS_EXP.1 is a major SFR to fulfill O.FAX.

O.FAX can be fulfilled by implementing this security functional requirement.

O.VALIDATION Software verification

O.VALIDATION is the security objective where the TOE provides procedures to self-verify executable code in the TSF. To fulfil this security objective, it is required to implement the following SFRs.

(1) FPT_TST_EXP.1

FPT_TST_EXP.1 ensures that a suite of self-tests is run at initial startup (and power-on) to verify the integrity of executable code in the TSF.

FPT_TST_EXP.1 is a major SFR to fulfill O.VALIDATION.

O.VALIDATION can be fulfilled by implementing this security functional requirement.

O.AUDIT Management of audit log records

O.AUDIT is the security objective to ensure that the TOE creates and maintains logs of TOE security-related events as audit log and protects them from disclosure or alteration by unauthorised persons, as well as provides audit logs in a format that can be verified by authorised persons. To fulfil this security objective, it is required to implement the following SFRs.

(1) FAU_GEN.1, FAU_GEN.2

FAU_GEN.1 and FAU_GEN.2 ensure that the events that should be audited are recorded together with the identification information of the cause of events that should be audited.

FAU_GEN.1 and FAU_GEN.2 are major SFRs to fulfill O.AUDIT.

(2) FAU_STG.1

FAU_STG.1 ensures that audit logs are protected from alteration.

FAU_STG.1 is a major SFR to fulfill O.AUDIT.

(3) FAU_STG.4

FAU_STG.4 ensures that the audit log with the oldest time stamp is deleted and a new audit log is recorded if an auditable event occurs while the audit log file is full.

FAU_STG.4 is an SFR that supports the fulfillment of O.AUDIT.

(4) FAU_SAR.1, FAU_SAR.2

FAU_SAR.1 ensures that audit logs can be read in a format that can be verified by the MFP administrator. FAU_SAR.2 ensures that anyone other than the MFP administrator is prohibited to read audit logs.

FAU_SAR.1 and FAU_SAR.2 are major SFRs to fulfill O.AUDIT.

(5) FPT_STM.1

FPT_STM.1 ensures that reliable time stamps are provided and the exact time when the audit event occurred is recorded to the audit log.

FPT_STM.1 is an SFR that supports the fulfillment of O.AUDIT.

(6) FIA_UID.1

FIA_UID.1 ensures that persons who attempt to use the TOE from the Operation Panel or the client computer on the network are identified.

FIA_UID.1 is an SFR that supports the fulfillment of O.AUDIT.

O.AUDIT can be fulfilled by implementing these security functional requirements.

O.EMMC_ENCRYPTION eMMC encryption

O.EMMC_ENCRYPTION is the security objective to ensure that data to be written to the eMMC is encrypted. To fulfil this security objective, it is required to implement the following SFRs.

(1) FCS_CKM.1

FCS_CKM.1 ensures that cryptographic keys are generated in accordance with a specified algorithm.

FCS_CKM.1 is an SFR that supports the fulfillment of O.EMMC_ENCRYPTION.

(2) FCS_CKM.4

FCS_CKM.4 ensures that cryptographic keys are deleted in accordance with a specified method.

FCS_CKM.4 is an SFR that supports the fulfillment of O.EMMC_ENCRYPTION.

(3) FCS_COP.1

FCS_COP.1 ensures that data to be written to the eMMC is encrypted in accordance with the specified algorithm and key sizes, and data read from the eMMC is decrypted.

FCS_COP.1 is a major SFR to fulfill O.EMMC_ENCRYPTION.

O.EMMC_ENCRYPTION can be fulfilled by implementing these security functional requirements.

6.3.3 Dependency Analysis

Table 27 describes the result of dependency analysis in this ST for the TOE security functional requirements.

Table 27: Results of Dependency Analysis of TOE Security Functional Requirements

TOE Security Functional Requirements	Claimed Dependencies	SFRs in this 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

TOE Security Functional Requirements	Claimed Dependencies	SFRs in this ST	Sufficiency
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
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	FDP_ACF.1	FDP_ACF.1	OK
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	OK
FDP_FXS_EXP.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
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	OK
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	OK However, since no interface is provided to modify user privileges, modify document data owner information, or modify user job data owner information, these management functions are not required for FMT_SMF.1.

TOE Security Functional Requirements	Claimed Dependencies	SFRs in this ST	Sufficiency
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 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 function is 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_EXP.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.

Based on the terms and costs of the evaluation, the evaluation assurance level of EAL2 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 in eMMC as 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 (Audit data generation)

The TOE records audit log items, shown in Table 29, in the eMMC when audit events shown in Table 28 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 29 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 28: List of Audit Events

Audit Events
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 24
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 Events
Deletion of user job data
Start and end of printing temporarily-saved document data, fax transmission documents, fax reception documents, stored print documents, and Document Server documents
Start and end of downloading scanned documents, fax transmission documents, and fax reception documents
Start and end of sending scanned documents by e-mail transmission of attachments
Start and end of sending scanned documents by folder transmission
Start and end of sending fax transmission documents by fax transmission
Deletion of temporarily-saved document data, scanned documents, fax transmission documents, fax reception documents, stored print documents, and Document Server documents

Table 29: List of Audit Log Data Items

	Audit Log Items	Setting Values of Audit Log Items	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 28
	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)	

	Audit Log Items	Setting Values of Audit Log Items	Audit Events to Record Audit Logs
Expanded Log Items	Job type	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 printing temporarily-saved document data, fax transmission documents, fax reception documents, stored print documents, and Document Server documents - Start and end of downloading scanned documents, fax transmission documents, and fax reception documents - Sending scanned documents by e-mail transmission of attachments - Sending scanned documents by folder transmission - Sending fax transmission documents by fax transmission - Deletion of temporarily-saved document data, scanned documents, fax transmission documents, fax reception documents, stored print documents, and Document Server documents - Deletion of user job data
	Login user name	All login user names that attempted the user identification	- Success and failure of login operations
	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 (User identity association)

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

FPT_STM.1 (Reliable time stamps)

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 (Audit review)

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.

FAU_SAR.2 (Restricted audit review)

The TOE does not provide an interface for downloading audit logs to all users except the MFP administrators.

FAU_STG.1 (Protected audit trail storage)

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 (Prevention of audit data loss)

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

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 (User authentication and identification)

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 (User-subject binding)

Based on the result of FIA_UAU.1 and FIA_UID.1, the TOE assigns the login user name and user privilege to processes performed by the authorised user.

FIA_ATD.1 (User attribute definition)

The TOE retains the login user name and user privilege based on settings for each user. User 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 (TSF-initiated termination)

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.

- For the Operation Panel, the user is logged out of the TOE automatically when the time that elapses since their final operation reaches the Operation Panel auto logout time (10 to 999 seconds).
- For the WIM, the user is logged out of the TOE automatically 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 (Protected authentication feedback)

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 (Authentication failure handling)

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 30, until an unlocking administrator releases the lockout
- For MFP administrators and supervisors, 60 seconds elapse since the MFP becomes executable after its power is turned on

Table 30 : Relationships regarding Lockout Release

Locked Out User	Unlocking Administrator
Normal user	MFP administrator
MFP administrator	Supervisor
Supervisor	MFP administrator

FIA_SOS.1 (Verification of secrets)

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 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] (10 digits)
- Symbols: SP (spaces) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ (33 symbols)

The conditions for registrable password length differ depending on normal users, MFP administrators, and supervisors, as shown below. The minimum character number of login password (i.e. minimum login 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 character number, and 128 characters or less

- For MFP administrators and supervisors: Equal to or longer than the minimum character number, and 32 characters or less

7.3 Document Access Control Function

The Document Access Control Function is to authorise 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.

FDP_ACC.1, FDP.ACF (Subset access control and Security attribute based access control)

The TOE provides the Document Access Control Function by enforcing the user data access control SFPs. Rules of user data access control SFPs are divided into (1) access control rules on document data and (2) access control rules on user job data. According to them, the TOE restricts operations on document data and user job data by users.

(1) **Access control rules on document data**

Table 31 describes the access control rules on document data. The TOE restricts the operations of deleting or reading document data to normal users, MFP administrators, and supervisors. No interface for modifying document data is provided. In particular, Table 32 describes the normal user operations, and no interface is provided for operations other than those described in Table 32.

Table 31: Access Control Rules on Document Data

User privilege	Document Data	Access Control Rule
Normal user	Temporarily-saved document data	Normal users who have the same login user name as that registered in the "document data owner information" of the temporarily-saved document data are allowed read and delete operations. Other normal users cannot display the document data in the list, and they are not allowed the read and delete operations.

User privilege	Document Data	Access Control Rule
	Scanned document Fax transmission document Stored print document Document Server document	Normal users who have the same login user name as that registered in the "document data owner information" are allowed read and delete operations. Normal users who have the same login user name as that registered in the "list of users who have been granted access permission for the document data" are allowed read operation. Other normal users cannot display the document data in the list, and they are not allowed the read and delete operations.
	Fax reception document	Normal users registered in the "fax reception document user" are allowed read and delete operations. Other normal users cannot display the document data in the list, and they are not allowed the read and delete operations.
MFP administrator	Temporarily-saved document Stored print document	MFP administrators are allowed the delete operation through the Operation Panel or WIM. No interface for reading document data is provided.
	Scanned document Fax transmission document Document Server document	MFP administrators are allowed the delete operation through the Operation Panel or WIM. MFP administrators are allowed the preview operation through the WIM. (No other interface for reading document data is provided.)
	Fax reception document	No interfaces for deleting and reading document data are provided.
Supervisor	Temporarily-saved document Scanned document Fax transmission document Stored print document Document Server document Fax reception document	No interfaces for deleting and reading document data are provided.

Table 32: Normal User Operations on Document Data

No.	Object	Operations	Operation Interface	MFP Application
1	Temporarily-saved document data	Delete Print Preview	Operation Panel	Printer Function
2	Temporarily-saved document data	Delete	WIM	Printer Function
3	Scanned document	Delete (*1) E-mail transmission of attachments Folder transmission Preview	Operation Panel	Scanner Function
4	Scanned document	Delete (*1) E-mail transmission of attachments Folder transmission Preview Download	WIM	Document Server Function
5	Fax transmission document	Delete (*1) Fax transmission Preview	Operation Panel	Fax Function
6	Fax transmission document	Delete (*1) Print Preview	Operation Panel	Document Server Function
7	Fax transmission document	Delete (*1) Fax transmission Preview Download	WIM	Document Server Function
8	Fax reception document	Delete (*1) Print Preview	Operation Panel	Fax Function

No.	Object	Operations	Operation Interface	MFP Application
9	Fax reception document	Delete Preview Download	WIM	Fax Function
10	Stored print document	Delete (*1) Print Preview	Operation Panel	Printer Function
11	Stored print document	Delete (*1)	WIM	Printer Function
12	Document Server document	Delete (*1) Print Preview	Operation Panel	Document Server Function
13	Document Server document	Delete (*1) Preview	WIM	Document Server Function

(*1) The document data owner is allowed to delete the document data. Other users who are allowed access (viewing) the document data by the owner are not allowed to delete the document data.

(2) **Access control rules on user job data**

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

No interface for modifying 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 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 (Inter-TSF trusted channel)

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 33 lists 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 33: Encrypted Communications Provided by the TOE

Communicating Devices	Encrypted Communications Provided by the TOE	
	Protocols	Cryptographic Algorithms
Client computer (*1)	TLS1.2	AES (128bits, 256bits)
	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 communication uses the printer driver or fax driver, the TLS version of the supporting protocol depends on the OS version of the client computer.

7.5 Stored Data Protection Function

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

FCS_CKM.1 (Cryptographic key generation)

The TOE generates a 256-bit eMMC cryptographic key using the CTR_DRBG (AES-128) algorithm when encrypting the eMMC 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 (Cryptographic key destruction)

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

FCS_COP.1 (Cryptographic operation)

The TOE encrypts the data to be written to/read from the eMMC before writing it and decrypts the data 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 Security Management Function

The Security Management Function is to control the operation of TSF data and the behaviour of the Security Functions based on the user privileges or the login user name. This function includes a function to maintain the role of operating the Security Management Function and associate the role with the user, and a function to set appropriate default values for the security attributes.

FMT_SMR.1 (Security roles)

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, FMT_MTD.1(a), FMT_MTD.1(b) (Specification of Management Function, Control of the behaviour of the Security Functions, Management of security attributes, Management of TSF data)

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.
- TOE restricts operations on the TSF data according to the role of the user. As shown in Table 34, it allows users who have user privilege corresponding to the role for which operations are allowed to operate the TSF Data.

Table 34: Management of TSF Data

Category	TSF Data	Operations	Roles (User Privileges) for Which Operations are Allowed	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 (*2) 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 privilege	Modify (*1)	None	None
	Document data owner information	Modify (*1)	None	None
	List of users who have been granted access permission for the document data	Modify	MFP administrator Document data owner (Normal user)	Operation Panel (*3) WIM
		Change_default	MFP administrator	Operation Panel WIM
	Fax reception document user	Modify	MFP administrator	Operation Panel WIM

Category	TSF Data	Operations	Roles (User Privileges) for Which Operations are Allowed	Operation Interface
	User job data owner information	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	Operation Panel WIM
		Query (*1)	None	None
	Login password [When associated with an MFP administrator]	Newly create	MFP administrator	Operation Panel WIM
		Modify	MFP administrator in question Supervisor	Operation Panel WIM
		Query (*1)	None	None
	Login password [When associated with a supervisor]	Modify	Supervisor	Operation Panel WIM
		Query (*1)	None	None
	eMMC cryptographic key	Query Delete Newly create	MFP administrator	Operation Panel

(*1): No interface is provided

(*2): 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.

(*3): For stored print document, the list of 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 (Static attribute initialisation)

Table 35 describes the list of static initialisation for security attributes, and Table 36 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 35 and Table 36 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 35: List of Static Initialisation for Security Attributes

Object	Security Attribute	Default Value	Overwriting Default Value
Document data	Document data owner information	See Table 36.	See Table 36.
	List of users who have been granted access permission for the document data	See Table 36.	See Table 36.
User job data	User job data owner information	Login user names of normal users who created the user job data	None

Table 36: Security Attributes for Each Case of Document Data Generation

Object Generation	Security Attribute	Default Value	Overwriting Default Value
Specify the print method as temporary saving print and temporarily save document data as temporarily-saved document from the printer driver.	Document data owner information	Login user names of normal users who created the document data	None
Specify the print method as stored print and store document data as stored print document from the printer driver.	Document data owner information	Login user names of normal users who created the document data	None
	List of users who have been granted access permission for the document data	Default values in the list of users who have been granted access permission for the document data (the list of login user names) for the document data creator	None
Specify the print method as Document Server storage and store	Document data owner information	Login user names of normal users who created the document data	None

Object Generation	Security Attribute	Default Value	Overwriting Default Value
document data as Document Server document from the printer driver.	List of users who have been granted access permission for the document data	Default values in the list of users who have been granted access permission for the document data (the list of login user names) for the document data creator	None
Store document data as fax transmission document from the fax driver.	Document data owner information	Login user names of normal users who created the document data	None
	List of users who have been granted access permission for the document data	Default values in the list of users who have been granted access permission for the document data (the list of login user names) for the document data creator	None
Scan a paper document and store it as Document Server document from the Operation Panel (Copy Function or Document Server Function).	Document data owner information	Login user names of normal users who created the document data	None
	List of users who have been granted access permission for the document data	Default values in the list of users who have been granted access permission for the document data (the list of login user names) for the document data creator	Values that the document data creator has allowed access (viewing) from the Operation Panel (the list of login user names) can be overwritten.
Scan a paper document and store it as scanned document from the Operation Panel (Scanner Function).	Document data owner information	Login user names of normal users who created the document data	None
	List of users who have been granted access permission for the document data	Default values in the list of users who have been granted access permission for the document data (the list of login user names) for the document data creator	Values that the document data creator has allowed access (viewing) from the Operation Panel (the list of login user names) can be overwritten.
Scan a paper document and store it as fax transmission document from	Document data owner information	Login user names of normal users who created the document data	None

Object Generation	Security Attribute	Default Value	Overwriting Default Value
the Operation Panel (Fax Function).	List of users who have been granted access permission for the document data	Default values in the list of users who have been granted access permission for the document data (the list of login user names) for the document data creator	Values that the document data creator has allowed access (viewing) from the Operation Panel (the list of login user names) can be overwritten.
Store document data received by fax via the telephone line as fax reception document.	Fax reception document user	List in which access to the fax reception document is set (the list of login user names)	None

7.7 Integrity Verification Function

The Integrity Verification Function is a self-test function that verifies the integrity of execution code in the MFP Control Software and the Operation Panel control software.

FPT_TST_EXP.1 (TSF testing)

The TOE performs the integrity verification of control software during the initial start-up.

By comparing the hash value or verifying digital signature for the MFP Control Software and the Operation Panel control software, the TOE verifies the integrity of control software.

If the hash value for the integrity verification obtained at startup does not match the correct value, or if the digital signature is not verified, the TOE will display an error message on the Operation Panel and will not accept the operation. If the obtained hash value matches the correct value and the digital signature is verified, the TOE will become available.

7.8 Fax Line Separation Function

The Fax Line Separation Function is to prohibit communication via a fax interface, except for transmission or reception of user data using a fax protocol, in order to prevent intrusion from the telephone line into the LAN.

FDP_FXS_EXP.1 (Fax separation)

By communicating only with the G3 standard on the telephone line and not using other communications, the TOE prohibits communication via a fax interface, except for transmission or reception of user data using a fax protocol.

8 Glossary

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

Table 37: Specific Terms Related to This ST

Terms	Definitions
MFP Control Software	A software component installed in the TOE. This is stored in the control board of the main unit.
Operation Panel Control Software	A software component installed in the TOE. This is stored in the Operation Panel Control Board.
Lockout	A type of behaviour to deny login of particular users.
Auto logout	A function for automatic user logout if no access is attempted from the Operation Panel or the WIM for the predetermined period of time.
eMMC	Abbreviation for Embedded Multi Media Card. A storage device that is non-volatile memory. In this document, unless otherwise specified, "eMMC" indicates the eMMC 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 functions provided by the TOE (Copy Function, Scanner Function, Printer Function, Document Server Function, Fax Transmission Function, and Fax Reception Function).
Operation Panel	A panel that consists of a touch screen LCD 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.
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.
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.
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.
Responsible manager of MFP	A person who is indirectly involved in the TOE and responsible for appointment of the TOE administrators in the organisation where the TOE is used.