



**RICOH IM 550/600/600SR, version E-1.20-H**

# **Security Target**

**Version 1.0**

**October 2024**

**Document prepared by**



[www.lightshipsec.com](http://www.lightshipsec.com)

## Document History

| Version | Date        | Description               |
|---------|-------------|---------------------------|
| 1.0     | 08 Oct 2024 | Release for certification |

## Table of Contents

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Introduction .....</b>                       | <b>5</b>  |
| 1.1      | Overview .....                                  | 5         |
| 1.2      | Identification .....                            | 5         |
| 1.3      | Conformance Claims.....                         | 5         |
| 1.4      | Terminology.....                                | 6         |
| <b>2</b> | <b>TOE Description .....</b>                    | <b>7</b>  |
| 2.1      | Type .....                                      | 7         |
| 2.2      | Usage .....                                     | 7         |
| 2.3      | Physical Scope.....                             | 9         |
| 2.4      | Logical Scope.....                              | 10        |
| <b>3</b> | <b>Security Problem Definition.....</b>         | <b>14</b> |
| 3.1      | Users .....                                     | 14        |
| 3.2      | Assets.....                                     | 14        |
| 3.3      | Threats .....                                   | 16        |
| 3.4      | Assumptions.....                                | 16        |
| 3.5      | Organizational Security Policies.....           | 17        |
| <b>4</b> | <b>Security Objectives.....</b>                 | <b>18</b> |
| <b>5</b> | <b>Security Requirements .....</b>              | <b>20</b> |
| 5.1      | Conventions .....                               | 20        |
| 5.2      | Extended Components Definition.....             | 20        |
| 5.3      | Functional Requirements .....                   | 21        |
| 5.4      | Assurance Requirements .....                    | 42        |
| <b>6</b> | <b>TOE Summary Specification.....</b>           | <b>43</b> |
| 6.1      | Security Audit .....                            | 43        |
| 6.2      | Identification and Authentication .....         | 44        |
| 6.3      | Access Control .....                            | 45        |
| 6.4      | Cryptographic Operations .....                  | 47        |
| 6.5      | Stored Data Encryption .....                    | 48        |
| 6.6      | Protection of the TSF .....                     | 49        |
| 6.7      | Trusted Communications .....                    | 49        |
| 6.8      | Administrative Roles .....                      | 51        |
| 6.9      | Trusted Operation .....                         | 52        |
| 6.10     | PSTN Fax-Network Separation.....                | 54        |
| 6.11     | Image Overwrite .....                           | 55        |
| <b>7</b> | <b>Rationale.....</b>                           | <b>56</b> |
| 7.1      | Conformance Claim Rationale .....               | 56        |
| 7.2      | Security Objectives Rationale .....             | 56        |
| 7.3      | Security Assurance Requirements rationale ..... | 58        |

## List of Tables

|   |    |
|---|----|
| Table 1: Evaluation identifiers .....   | 5  |
| Table 2: NIAP Technical Decisions ..... | 5  |
| Table 3: Terminology .....              | 6  |
| Table 4: TOE Models.....                | 9  |
| Table 5: CAVP Certificates.....         | 11 |
| Table 6: User Categories.....           | 14 |

Table 7: Asset Categories ..... 14

Table 8: User Data Types..... 14

Table 9: Document and Job Attributes ..... 15

Table 10: TSF Data Types ..... 15

Table 11: Threats..... 16

Table 12: Assumptions ..... 17

Table 13: Organizational Security Policies ..... 17

Table 14: Security Objectives for the TOE ..... 18

Table 15: Security Objectives for the Operational Environment ..... 19

Table 16: Extended Components ..... 20

Table 17: Summary of SFRs ..... 21

Table 18: Audit Events ..... 23

Table 19: D.USER.DOC Access Control SFP ..... 29

Table 20: D.USER.JOB Access Control SFP ..... 31

Table 21: Management of TSF Data ..... 36

Table 22: Management Functions ..... 37

Table 23: TOE Security Assurance Requirements..... 42

Table 24: List of Audit Events ..... 43

Table 25: Stored Documents Access Control Rules for Normal Users ..... 46

Table 26: Random Number Sources ..... 47

Table 27: Keychain encryption ..... 48

Table 28: TLS/HTTPS Cryptographic Functions ..... 50

Table 29: IPsec Cryptographic Functions ..... 51

Table 30: Start-up Integrity Tests ..... 53

Table 31: Signature Verification ..... 54

Table 32: Security Objectives Rationale ..... 56

# 1 Introduction

## 1.1 Overview

1 This Security Target (ST) defines the RICOH IM 550/600/600SR, version E-1.20-H Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

## 1.2 Identification

**Table 1: Evaluation identifiers**

|                             |  |
|-----------------------------|--|
| <b>Target of Evaluation</b> | RICOH IM 550/600/600SR, version E-1.20-H                       |
| <b>Security Target</b>      | RICOH IM 550/600/600SR, version E-1.20-H Security Target, v1.0 |

2 **Note:** The TOE version (E-1.20-H) is the collection of an alternative set of firmware packages. The complete list of firmware packages and versions can be found in Section 1.3.2 of the CC Guide.

## 1.3 Conformance Claims

3 This ST supports the following conformance claims:

- a) CC version 3.1 revision 5
- b) CC Part 2 extended
- c) CC Part 3 conformant
- d) Protection Profile for Hardcopy Devices, v1.0
- e) Protection Profile for Hardcopy Devices, v1.0, Errata #1, June 2017
- f) NIAP Technical Decisions per Table 2

**Table 2: NIAP Technical Decisions**

| TD #   | Name   | Rationale if n/a           |
|--------|--|----------------------------|
| TD0157 | FCS_IPSEC_EXT.1.1 - Testing SPDs                   |                            |
| TD0176 | FDP_DSK_EXT.1.2 - SED Testing                      |                            |
| TD0219 | NIAP Endorsement of Errata for HCD PP v1.0         |                            |
| TD0253 | Assurance Activities for Key Transport             | FCS_COP.1.1(i) not claimed |
| TD0261 | Destruction of CSPs in flash                       |                            |
| TD0299 | Update to FCS_CKM.4 Assurance Activities           |                            |
| TD0393 | Require FTP_TRP.1(b) only for printing             |                            |
| TD0474 | Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1 |                            |

| TD #   | Name  | Rationale if n/a       |
|--------|---|------------------------|
| TD0494 | Removal of Mandatory SSH Ciphersuite for HCD                              | SSH is not claimed.    |
| TD0562 | Test activity for Public Key Algorithms                                   | SSH is not claimed.    |
| TD0642 | FCS_CKM.1(a) Requirement; P-384 keysize moved to selection                |                        |
| TD0844 | Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim | ALC_FLR is not claimed |

## 1.4 Terminology

**Table 3: Terminology**

| Term          | Definition   |
|---------------|--|
| BEV           | Border Encryption Value  |
| Firewall      | A device to protect the LAN from internet threats.   |
| FTP Server    | An external IT entity used by the TOE to receive and store user documents  |
| HDD           | A field-replaceable non-volatile memory storage device, that the TOE uses to store documents, and user accounts information. |
| LAN           | Local Area Network — Network used in the TOE environment   |
| Ic key        | A hardware secure module which provides true random number generation and protected storage for the TOE.                     |
| LDAP Server   | An external IT entity used by the TOE for network authentication of users.   |
| MFP           | Multifunction Printer  |
| NVRAM         | The NVRAM is a field-replaceable non-volatile storage device where TOE configuration data is stored.                         |
| PSTN          | Public Switched Telephone Network  |
| PSTN Line     | A connection to a public switched telephone network for the TOE to communicate with external fax machines                    |
| SMTP Server   | An external IT entity used by the TOE for e-mail transmission  |
| Syslog Server | An external IT entity used by the TOE for audit log storage  |

## 2 TOE Description

### 2.1 Type

4 The TOE is a Digital Multi-Function Printer (MFP), which is an IT device that inputs, stores, and outputs electronic and hardcopy documents.

### 2.2 Usage

5 The expected use cases for the TOE are:

- a) **Scanning.** The TOE scans paper documents and then transmits and deletes the scanned images, on command from the Operation Panel.
- b) **Printing.** The TOE prints or stores documents received from a printer driver installed on the client computer, and prints or deletes previously-stored documents from commands from the Operation Panel or the client computer's web browser
- c) **Copying.** The TOE scans paper documents to be printed.
- d) **Network Communications.** The TOE is connected to its operational environment through a local area network (hereafter "LAN") and the public switched telephone network (PSTN). It sends and receives documents over the LAN and the PSTN.
- e) **Administration.** The TOE provides management functions to configure and manage its operation. The management functions are accessible locally from the Operation Panel or remotely through the Web Image Monitor (hereafter "WIM") accessible using a web browser on a client computer.
- f) **PSTN Faxing.** The TOE provides fax transmission and fax reception functions; both exchange documents according to the Group 3 standard over a Public Switch Telephone Network (PSTN). The Fax Transmission Function sends scanned images of paper documents, or images of electronic documents from a client computer, to external fax devices. The Fax Reception Function receives documents from external fax devices, and stores them in the TOE
- g) **Storage and Retrieval.** The TOE provides a Document Server Function which stores documents and allows users to perform operations on persistently-stored documents. From the operation panel, users can store, print and delete documents stored by the document server. From a client computer, users can print and delete documents stored by the document server.
- h) **Field-Replaceable Non-volatile Storage.** The TOE stores encrypted data both in the HDD and in NVRAM.
- i) **Internal Audit Log Storage.** The MFP stores its audit data internally on the local device in addition to providing the capability for storing them externally to a remote syslog server.
- j) **Image Overwrite.** The MFP actively overwrites residual image data stored on the HDD after a document processing job has been completed or cancelled.

## 2.2.1 Deployment

- 6 As shown in Figure 1, the TOE is connected to its operational environment through a local area network (hereafter "LAN") and the public switched telephone network (PSTN). Other elements of the TOE's operational environment include a remote fax machine, an SMTP server, an Audit Server, and a user's client computer.

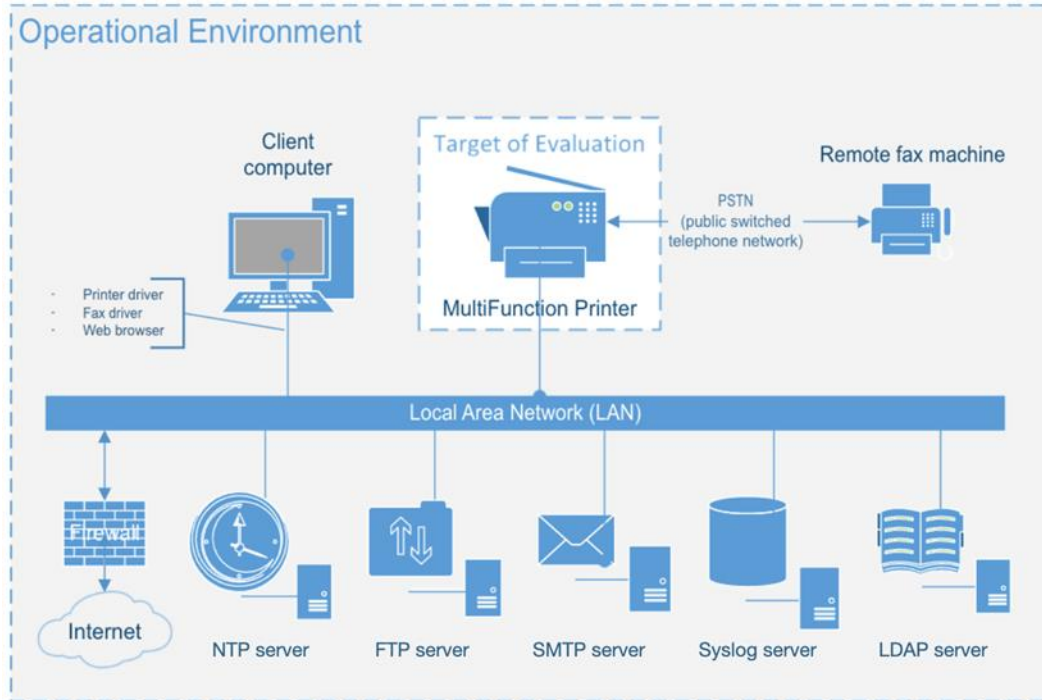


Figure 1: Example TOE deployment

## 2.2.2 Interfaces

- 7 The TOE interfaces include the following:
- a) **Operation Panel of the MFP** is an LCD touch screen interface that provides a local user interface where users can perform the following operations:
    - i. Configuration of the MFP
    - ii. Copying, faxing, storage, and network transmission of paper documents
    - iii. Printing, faxing, network transmission, and deletion of the stored documents
    - iv. Receiving fax documents via telephone lines and storing them
  - b) **Web Image Monitor (WIM)** this is the remote user interface accessible via TLS/HTTPS where users can perform the following operations:
    - i. Limited configuration of the MFP – various settings
    - ii. Operation on stored documents
    - iii. Storage and/or printing of documents
    - iv. Faxing of documents
  - c) **Client printer driver or fax driver** is a remote user interface where communication is protected using TLS.



- d) **IPSec interface** is used by the TOE to communicate with LDAP, syslog, NTP, SMTP and FTP servers in the TOE operational environment.
- e) **TLS interface:** The TOE can be configured to also use TLS to protect communication with a remote syslog, SMTP server, and LDAP server.
- f) **PSTN Fax Line** is used to connect to a remote fax machine.

### 2.3 Physical Scope

- 8 The physical boundary of the TOE is comprised of the software and hardware of the MFP models identified in Table 4(which shows the different RICOH Family Group brand names for the TOE) and related guidance documentation. The TOE is delivered by commercial courier and is installed with the assistance of a RICOH customer engineer.
- 9 The TOE model number is indicative of copy speed (higher numbers have higher copy speeds). The differences between models are not security relevant and are limited to print engine components (speed) and branding variations (labels, displays, packaging materials and documentation).

**Table 4: TOE Models**

| Branding   | Model   |
|------------|---|
| RICOH      | IM 550F<br>IM 600F<br>IM 600SRF<br>IM 600SRFG |
| nashuatec  | IM 550F<br>IM 600F<br>IM 600SRF               |
| Rex Rotary | IM 550F<br>IM 600F<br>IM 600SRF               |
| Gestetner  | IM 550F<br>IM 600F<br>IM 600SRF               |

- 10 The TOE includes the following critical components:
- a) **Main Controller.** Provides primary printing, scanning, faxing, and networking functionality.
    - i) **CPU.** Intel Goldmont CPU:
      - Intel Atom x5-E3930
    - ii) **OS.** LPUX6.0 OS (customized NetBSD 6.0.1).
  - b) **Operation Unit.** Provides front panel interface control and device extensibility capabilities.
    - i) **CPU.** ARM Cortex-A9 Quad Core.
    - ii) **OS.** Linux 3.18 (customized).

### 2.3.1 Guidance Documents

- 11 The TOE guidance documentation shown below is available through the vendor's support portal. The Common Criteria Guide is provided by the vendor upon request.
- a) [User Guide IM 550/600 Series](#), D0BW7316
  - b) [Security Guide](#), D0BW7328 2024.02
  - c) [Security Reference](#), D0E37534-EN 2023/2
  - d) RICOH IM 550/600/600SR Common Criteria Guidance, v2.1 (PDF)

## 2.4 Logical Scope

- 12 The logical scope of the TOE comprises the security functions provided by the TOE to include:
- a) **Security Audit.** The TOE generates audit records of user and administrator actions. It stores audit records both locally and on a remote syslog server.
  - b) **Cryptographic Support.** The TOE includes a cryptographic module for the cryptographic operations that it performs. The relevant CAVP certificate numbers are noted in Table 5 below.
  - c) **Access Control.** The TOE enforces access control policy to restrict access to user data. The TOE ensures that documents, document processing job information, and security-relevant data are accessible only to authenticated users who have the appropriate access permissions.
  - d) **Storage Data Encryption.** The TOE encrypts data on the HDD and in NVRAM to protect documents and confidential system information if those devices are removed from the TOE.
  - e) **Identification and Authentication.** Except for a defined minimal set of actions that can be performed by an unauthenticated user, the TOE ensures that all users must be authenticated before accessing its functions and data. Users login to the TOE by entering their credentials on the local operation panel, through WIM login, through print or fax drivers, or using network authentication services.
  - f) **Administrative Roles.** The TOE provides the capability for managing its functions and data. Role-based access controls ensure that the ability to configure the security settings of the TOE is available only to the authorized administrators. Authenticated users can perform copy, printer, scanner,

document server and fax operations based on the user role and the assigned permissions.

- g) **Trusted Operations.** The TOE performs power-on self-tests to ensure the integrity of the TSF components. It provides a mechanism for performing trusted update that verifies the integrity and authenticity of the upgrade software before applying the updates. It uses an NTP server for accurate time.
- h) **TOE Access.** Interactive user sessions at the local and remote user interfaces are automatically terminated by the TOE after a configured period of inactivity.
- i) **Trusted Communications.** The TOE protects communications from its remote users using TLS/HTTPS, and communications with the LDAP, FTP, SMTP, Syslog, SMTP, and NTP servers using IPsec. Optionally, the TOE can also be configured to protect communications with Syslog, LDAP and SMTP servers using TLS.
- j) **PSTN Fax-Network Separation.** The TOE restricts information received from or transmitted to the telephone network to only fax data and fax protocols. It ensures that the fax modem cannot be used to bridge the LAN.
- k) **Image Overwrite.** the TOE actively overwrites residual image data stored on the HDD after a document processing job has been completed or cancelled.

## 2.4.1 CAVP Certificates

13 The TOE includes the cryptographic modules with related CAVP certificates shown Table 5 below.

**Table 5: CAVP Certificates**

| Cryptographic Module                               | Operating Environment                                    | Algorithms                                      | CAVP #    |
|--|--|---|-----------|
| RICOH Cryptographic Module for IPsec, version 1.00 | Customized NetBSD 6.0.1 on Intel Atom X5-E3930 processor | AES-CBC   | AES 5315  |
|  |  | SHA-256<br>SHA-384<br>SHA-512                   | SHS 4269  |
|  |  | HMAC-SHA2_256<br>HMAC-SHA2-384<br>HMAC-SHA2-512 | HMAC 3515 |
| RICOH Platform Validation Library for JX3          | BIOS on Intel Atom x5-E3930 processor                    | SHA-1   | C630      |
| RICOH Cryptographic Library 2 (Java), v1.0         | Customized Linux 3.18 on ARM Cortex-A9 Quad Core         | SHA-1<br>SHA2-256<br>RSA Signature Verification | C582      |
| libgwwguard, v0.9.8a                               |  | SHA2-256  | SHS 3231  |

| Cryptographic Module                         | Operating Environment  | Algorithms   | CAVP #   |
|--|--|--|----------|
|  | Customized NetBSD 6.0.1 on Intel Atom x5-E3930                     | RSA Signature Verification   | RSA 2002 |
| RICOH Cryptographic Library C, v1.2          | Customized Linux 3.18 on ARM Cortex-A9 Quad Core Processor         | Curve P-256<br>SHA2-256  | C629     |
| LPUX NVRAM Encryption Driver, v1.2           | Customized NetBSD 6.0.1 on Intel Atom X5-E3930 processor           | AES-CBC<br>Encryption/decryption<br>Key length: 256  | AES 4560 |
| Boot SHA-1 Module                            | Firmware version 47.04<br>Processor:<br>ST33TPHF2ESPI              | SHA-1  | C715     |
| RICOH Company<br>AES256CBC<br>Implementation | MB8AL1062MH-GE1<br>Hardware  | AES-CBC<br>Encrypt, Decrypt<br>Key Length: 256   | AES 3921 |
| WolfCrypt, version 3.14.2a                   | NetBSD v6.0.1 on Intel Atom Apollo Lake E3930 (Goldmont) Processor | RSA Key Generation<br>RSA Signature Generation (PKCS 1.5)<br>RSA Signature Verification (PKCS 1.5) | A5250    |
|  |  | SHA-1, SHA-256, SHA-384, SHA-512   |          |
|  |  | AES-CBC<br>AES-GCM<br>Encryption/decryption<br>Key length 128, 256                                 |          |
|  |  | HMAC-SHA-1<br>HMAC-SHA2-256<br>HMAC-SHA2-384<br>HMAC-SHA2-512                                      |          |
|  |  | DRBG   |          |
|  |  | KAS-ECC  |          |
|  |  | KAS-FFC  |          |

## 2.4.2 Excluded Features

14 The following Features of the MFP are excluded from the evaluated configuration:

- a) **USB Port.** The MFP has a USB Port that is used to directly connect a client computer to the MFP for printing. This USB port is disabled during initial installation and configuration of the TOE.
- b) **SD Card Slot.** The MFP has two SD Card Slots, one for customer engineers and one for users. The SD Card Slot for customer engineer is used by customer engineers to install components of the MFP; the SD Card Slot for users is used by users to print documents. Both are disabled when the TOE is operational, a cover is placed on the SD Card slot for customer engineer so cards cannot be inserted or removed and the card slot for users is set to disabled during installation.

## 2.4.3 Required non-TOE Components

15 The following non-TOE components are required in the TOE operational environment:

- a) **Syslog Server.** The TOE uses a remote syslog server for long term storage of its audit trail.
- b) **LDAP Server.** The TOE uses an LDAP server for user authentication.
- c) **NTP Server.** The TOE ensures accurate time by synchronizing with a remote NTP server.
- d) **FTP Server.** The TOE stores user documents on a remote FTP server.
- e) **SMTP Server.** The TOE uses an SMTP server for email transmission.

### 3 Security Problem Definition

16 The Security Problem Definition is reproduced from section 2 of the HCDPP.

#### 3.1 Users

17 There are two categories of Users defined in this ST, Normal and Admin.

**Table 6: User Categories**

| Designation | Name          | Definition  |
|-------------|---------------|---|
| U.NORMAL    | Normal User   | A User who has been identified and authenticated and does not have an administrative role |
| U.ADMIN     | Administrator | A User who has been identified and authenticated and has an administrative role           |

18 A pseudo-user role, Customer Engineer, can be enabled by an Administrator for use by an authorized service representative. It is normally disabled, as it is in the evaluated configuration.

#### 3.2 Assets

19 Assets are passive entities in the TOE that contain or receive information. In this PP, Assets are Objects (as defined by the CC). There are two categories of Assets defined in this PP:

**Table 7: Asset Categories**

| Designation | Asset category | Definition   |
|-------------|----------------|--|
| D.USER      | User Data      | Data created by and for Users that do not affect the operation of the TSF  |
| D.TSF       | TSF Data       | Data created by and for the TOE that might affect the operation of the TSF |

20 There are no additional Asset categories defined in this ST.

##### 3.2.1 User Data

21 User Data are composed of two types:

**Table 8: User Data Types**

| Designation | User Data type     | Definition   |
|-------------|--------------------|--|
| D.USER.DOC  | User Document Data | Information contained in a User's Document, in electronic or hardcopy form |
| D.USER.JOB  | User Job Data      | Information related to a User's Document or Document Processing Job        |

22 There are no additional types of User Data defined in this ST. Attributes associate documents and document processing jobs with the document processing functions of the TOE:

**Table 9: Document and Job Attributes**

| Document processing function | Attribute |
|------------------------------|-----------|
| Printing                     | +PRT      |
| Copying                      | +CPY      |
| Scanning                     | +SCN      |
| Document Storage/Retrieval   | +DSR      |
| Fax (reception)              | +FAXIN    |
| Fax (transmission)           | +FAXOUT   |

**3.2.2 TSF Data**

23 TSF Data are composed of two types:

**Table 10: TSF Data Types**

| Designation | TSF Data type         | Definition  |
|-------------|-----------------------|---|
| D.TSF.PROT  | Protected TSF Data    | TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable |
| D.TSF.CONF  | Confidential TSF Data | TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE                    |

24 There are no additional types of TSF Data defined in this ST.

**3.2.2.1 Protected TSF Data**

25 D.TSF.PROT is composed of the following data:

- a) Login user name
- b) Number of Attempts before Lockout
- c) Settings for Lockout Release Timer
- d) Lockout time
- e) Date settings (year/month/day)
- f) Time settings
- g) Minimum Character No.
- h) Password Complexity Setting

- i) Operation Panel auto logout time
- j) WIM auto logout time
- k) Stored Reception File User
- l) Document user list
- m) Available function list
- n) User authentication method
- o) Device Certificate
- p) Network settings
- q) Audit transfer settings
- r) TOE Software

**3.2.2.2 Confidential TSF Data**

26 D.TSF.CONF is composed of the following data:

- a) Login password
- b) Audit log
- c) HDD cryptographic key

**3.3 Threats**

27 The following threats are mitigated by this TOE:

**Table 11: Threats**

| Identifier             | Description  |
|------------------------|--|
| T.UNAUTHORIZED_ACCESS  | An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces. |
| T.TSF_COMPROMISE       | An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.   |
| T.TSF_FAILURE          | A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.  |
| T.UNAUTHORIZED_UP DATE | An attacker may cause the installation of unauthorized software on the TOE.  |
| T.NET_COMPROMISE       | An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.                    |

**3.4 Assumptions**

28 The following assumptions must be satisfied in order for the Security Objectives and Security Functional Requirements to be effective:



**Table 12: Assumptions**

| Identifier      | Description  |
|-----------------|--|
| A.PHYSICAL      | Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment. |
| A.NETWORK       | The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.                                   |
| A.TRUSTED_ADMIN | TOE Administrators are trusted to administer the TOE according to site security policies.  |
| A.TRAINED_USERS | Authorized Users are trained to use the TOE according to site security policies.   |

### 3.5 Organizational Security Policies

29 The following Organizational Security Policies (OSPs) are enforced by this TOE:

**Table 13: Organizational Security Policies**

| Identifier           | Description   |
|----------------------|---|
| P.AUTHORIZATION      | Users must be authorized before performing Document Processing and administrative functions.  |
| P.AUDIT              | Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.  |
| P.COMMS_PROTECTION   | The TOE must be able to identify itself to other devices on the LAN.  |
| P.STORAGE_ENCRYPTION | If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.   |
| P.KEY_MATERIAL       | Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device. |
| P.FAX_FLOW           | If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.   |
| P.IMAGE_OVERWRITE    | Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.   |

## 4 Security Objectives

30 The following Security Objectives are satisfied by this TOE:

**Table 14: Security Objectives for the TOE**

| Identifier            | Description  |
|-----------------------|--|
| O.USER_I&A            | The TOE shall perform identification and authentication of Users for operations that require access control, User authorization, or Administrator roles.   |
| O.ACCESS_CONTROL      | The TOE shall enforce access controls to protect User Data and TSF Data in accordance with security policies.  |
| O.USER_AUTHORIZATION  | The TOE shall perform authorization of Users in accordance with security policies.   |
| O.ADMIN_ROLES         | The TOE shall ensure that only authorized Administrators are permitted to perform administrator functions.   |
| O.UPDATE_VERIFICATION | The TOE shall provide mechanisms to verify the authenticity of software updates.   |
| O.TSF_SELF_TEST       | The TOE shall test some subset of its security functionality to help ensure that subset is operating properly.   |
| O.COMMS_PROTECTION    | The TOE shall generate audit data, and be capable of sending it to a trusted External IT Entity. Optionally, it may store audit data in the TOE.   |
| O.AUDIT               | The TOE shall generate audit data, and be capable of sending it to a trusted External IT Entity. Optionally, it may store audit data in the TOE.   |
| O.STORAGE_ENCRYPTION  | If the TOE stores User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage devices, then the TOE shall encrypt such data on those devices.   |
| O.KEY_MATERIAL        | The TOE shall protect from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Field-Replaceable Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material. |
| O.FAX_NET_SEPARATION  | If the TOE provides a PSTN fax function, then the TOE shall ensure separation of the PSTN fax telephone line and the LAN, by system design or active security function.  |
| O.IMAGE_OVERWRITE     | Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.  |

31 The following Security Objectives must be satisfied by the TOE's Operational Environment.

**Table 15: Security Objectives for the Operational Environment**

| Identifier             | Description  |
|------------------------|--|
| OE.PHYSICAL_PROTECTION | The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes.   |
| OE.NETWORK PROTECTION  | The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface.   |
| OE.ADMIN_TRUST         | The TOE Owner shall establish trust that Administrators will not use their privileges for malicious purposes.  |
| OE.USER_TRAINING       | The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them.  |
| OE.ADMIN_TRAINING      | The TOE Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer's guidance to correctly configure the TOE and protect passwords and keys accordingly. |

## 5 Security Requirements

### 5.1 Conventions

32 This document uses the following font conventions to identify the operations defined by the CC:

- c) **Assignment.** Indicated with italicized text.
- 33 **Refinement.** Indicated with bold text and strikethroughs.
- d) **Selection.** Indicated with underlined text.
- e) **Assignment within a Selection:** Indicated with italicized and underlined text.
- f) **Iteration.** Indicated by adding letter in parentheses for iterations completed in the PP. Iterations completed in the ST are identified by adding a string starting “/” (e.g. “FCS\_CKM.1(b)/DIM”

**Note:** operations performed within the Security Target are denoted within brackets []. Operations shown without brackets are reproduced from the HCDPP.

### 5.2 Extended Components Definition

34 Table 16 identifies the Extended Components used in this ST, their source PP, and any related technical decisions

**Table 16: Extended Components**

| Extended SFR    | Source PP                               | Technical Decisions |
|-----------------|---|---------------------|
| FAU_STG_EXT.1   | Protection Profile for Hardcopy Devices |                     |
| FCS_CKM_EXT.4   | Protection Profile for Hardcopy Devices |                     |
| FCS_HTTPS_EXT.1 | Protection Profile for Hardcopy Devices |                     |
| FCS_IPSEC_EXT.1 | Protection Profile for Hardcopy Devices | TD0157              |
| FCS_KYC_EXT.1   | Protection Profile for Hardcopy Devices |                     |
| FCS_RBG_EXT.1   | Protection Profile for Hardcopy Devices |                     |
| FCS_TLS_EXT.1   | Protection Profile for Hardcopy Devices | TD0474              |
| FDP_DSK_EXT.1   | Protection Profile for Hardcopy Devices | TD0176              |
| FDP_FXS_EXT.1   | Protection Profile for Hardcopy Devices |                     |
| FIA_PMG_EXT.1   | Protection Profile for Hardcopy Devices |                     |
| FIA_PSK_EXT.1   | Protection Profile for Hardcopy Devices |                     |
| FPT_KYP_EXT.1   | Protection Profile for Hardcopy Devices |                     |
| FPT_SKP_EXT.1   | Protection Profile for Hardcopy Devices |                     |

| Extended SFR  | Source PP                               | Technical Decisions |
|---------------|---|---------------------|
| FPT_TST_EXT.1 | Protection Profile for Hardcopy Devices |                     |
| FPT_TUD_EXT.1 | Protection Profile for Hardcopy Devices |                     |

### 5.3 Functional Requirements

**Table 17: Summary of SFRs**

| Requirement      | Title  |
|------------------|--|
| FAU_GEN.1        | Audit Data Generation  |
| FAU_GEN.2        | User Identity Association  |
| FAU_SAR.1        | Audit Review   |
| FAU_SAR.2        | Restricted Audit Review  |
| FAU_STG.1        | Protected Audit Trail Storage                                      |
| FAU_STG_EXT.1    | Extended: External Audit Trail Storage                             |
| FAU_STG.4        | Prevention of Audit Data Loss                                      |
| FCS_CKM.1(a)     | Cryptographic Key Generation (for asymmetric keys)                 |
| FCS_CKM.1(b)/DAR | Cryptographic Key Generation (for Symmetric keys) [Data At Rest]   |
| FCS_CKM.1(b)/DIM | Cryptographic Key Generation (for Symmetric keys) [Data In Motion] |
| FCS_CKM_EXT.4    | Extended: Cryptographic Key Material Destruction                   |
| FCS_CKM.4        | Cryptographic Key Destruction                                      |
| FCS_COP.1(a)     | Cryptographic Operation (Symmetric Encryption/Decryption)          |
| FCS_COP.1(b)     | Cryptographic Operation (Signature Generation and Verification)    |
| FCS_COP.1(c)/L1  | Cryptographic Operation (Hash Algorithm)                           |
| FCS_COP.1(c)/L2  | Cryptographic Operation (Hash Algorithm)                           |
| FCS_COP.1(d)     | Cryptographic Operation (AES Data Encryption/Decryption)           |
| FCS_COP.1(f)     | Cryptographic Operation (Key Encryption)                           |

| Requirement     | Title   |
|-----------------|---|
| FCS_COP.1(g)    | Cryptographic Operation (for keyed-hash message authentication) |
| FCS_HTTPS_EXT.1 | Extended: HTTPS selected  |
| FCS_IPSEC_EXT.1 | Extended: IPsec selected  |
| FCS_KYC_EXT.1   | Extended: Key Chaining  |
| FCS_RBG_EXT.1   | Extended: Cryptographic Operation (Random Bit Generation)       |
| FCS_TLS_EXT.1   | Extended: TLS selected  |
| FDP_ACC.1       | Subset Access Control   |
| FDP_ACF.1       | Security attribute based access control                         |
| FDP_DSK_EXT.1   | Extended: Protection of Data on Disk                            |
| FDP_FXS_EXT.1   | Extended: Fax separation  |
| FDP_RIP.1(a)    | Subset residual information protection                          |
| FIA_AFL.1       | Authentication failure handling                                 |
| FIA_ATD.1       | User attribute definition                                       |
| FIA_PMG_EXT.1   | Extended: Password Management                                   |
| FIA_PSK_EXT.1   | Extended: Pre-Shared Key Composition                            |
| FIA_UAU.1       | Timing of authentication  |
| FIA_UAU.7       | Protected Authentication Feedback                               |
| FIA_UID.1       | Timing of identification  |
| FIA_USB.1       | User-subject binding  |
| FMT_MOF.1       | Management of security functions behavior                       |
| FMT_MSA.1       | Management of security attributes                               |
| FMT_MSA.3       | Static attribute initialization                                 |
| FMT_MTD.1       | Management of TSF Data  |
| FMT_SMF.1       | Specification of Management Functions                           |
| FMT_SMR.1       | Security roles  |

| Requirement     | Title  |
|-----------------|--|
| FPT_KYP_EXT.1   | Extended: Protection of Key and Key Material |
| FPT_SKP_EXT.1   | Extended: Protection of TSF Data             |
| FPT_STM.1       | Reliable Time Stamps                         |
| FPT_TST_EXT.1   | Extended: TSF testing                        |
| FPT_TUD_EXT.1   | Extended: Trusted update                     |
| FTA_SSL.3       | TSF-initiated Termination                    |
| FTP_ITC.1/TLS   | Inter-TSF trusted channel                    |
| FTP_ITC.1/IPSEC | Inter-TSF trusted channel                    |
| FTP_TRP.1(a)    | Trusted Path (for Administrators)            |
| FTP_TRP.1(b)    | Trusted Path (for Non-administrators)        |

**5.3.1 Security Audit (FAU)**

**FAU\_GEN.1 Audit Data Generation**

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

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the not specified level of audit;
- c) All auditable events specified in Table 18, [*no other auditable events*].

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, **additional information specified in-Table 18**, [*no other audit relevant information*].

**Table 18: Audit Events**

| Auditable Event                  | Relevant SFR | Additional information |
|----------------------------------|--------------|------------------------|
| Job completion                   | FDP_ACF.1    | Type of Job            |
| Unsuccessful User authentication | FIA_UAU.1    | None                   |

| Auditable Event  | Relevant SFR                             | Additional information |
|--|--|------------------------|
| Unsuccessful User identification                           | FIA_UID.1                                | None                   |
| Use of management functions                                | FMT_SMF.1                                | None                   |
| Modification to the group of Users that are part of a role | FMT_SMR.1                                | None                   |
| Changes to the time  | FPT_STM.1                                | None                   |
| Failure to establish session                               | FTP_ITC.1, FTP_TRP.1(a),<br>FTP_TRP.1(b) | Reason for failure     |

**FAU\_GEN.2****User Identity Association**

FAU\_GEN.2.1

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

**FAU\_SAR.1****Audit Review**

FAU\_SAR.1.1

The TSF shall provide [*U.ADMIN*] with the capability to read **all records** from the audit records.

FAU\_SAR.1.2

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

**FAU\_SAR.2****Restricted 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.

**FAU\_STG.1****Protected Audit Trail Storage**

FAU\_STG1.1

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

FAU\_STG1.2

The TSF shall be able to **prevent** unauthorised modifications to the stored audit records in the audit trail.

**FAU\_STG\_EXT.1****Extended: External Audit Trail Storage**

FAU\_STG\_EXT.1.1

The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP\_ITC.1.

**FAU\_STG.4****Prevention of Audit Data Loss**



FAU\_STG.4.1 Refinement The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.

### 5.3.2 Cryptographic Support (FCS)

#### FCS\_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

FCS\_CKM.1.1(a) Refinement The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance with [

- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes
- NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" [P256] (as defined in FIPS PUB 186-4, "Digital Signature Standard")

]

**and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.**

Note: This SFR was altered by TD0642.

#### FCS\_CKM.1(b)/DAR Cryptographic Key Generation (Symmetric keys)/Data At Rest

FCS\_CKM.1.1(b)/DAR Refinement The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS\_RBG\_EXT.1 and specified cryptographic key sizes [256 bit] that meet the following: No Standard.**

#### FCS\_CKM.1(b)/DIM Cryptographic Key Generation (Symmetric keys)/Data In Motion

FCS\_CKM.1.1(b)/DIM Refinement The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS\_RBG\_EXT.1 and specified cryptographic key sizes [128 bit, 256 bit] that meet the following: No Standard.**

#### FCS\_CKM\_EXT.4 Extended: Cryptographic Key Material Destruction

FCS\_CKM\_EXT.4.1 The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.

#### FCS\_CKM.4 Cryptographic Key Destruction

FCS\_CKM.4.1 Refinement The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

- For volatile memory, the destruction shall be executed by [selection: removal of power to the memory];
- For nonvolatile storage, the destruction shall be executed by a [single] overwrite consisting of [a new value of a key of the same size];

] that meets the following: No Standard.

Application Note: This SFR is altered by TD0261.

### **FCS\_COP.1(a) Cryptographic Operation (Symmetric Encryption/Decryption)**

FCS\_COP.1.1(a) Refinement The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in [CBC mode, GCM mode]** and cryptographic key sizes **128-bits and 256-bits** that meets the following:

- **FIPS PUB 197, “Advanced Encryption Standard (AES)”**
- **[NIST SP 800-38A, NIST SP 800-38D]**

### **FCS\_COP.1(b) Cryptographic Operation (for Signature Generation/Verification)**

FCS\_COP.1.1(b) Refinement The TSF shall perform **cryptographic signature services** in accordance with a [

- RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [2048 bits]

that meets the following: [

Case: RSA Digital Signature Algorithm:

- FIPS PUB 186-4, “Digital Signature Standard”]

Note: This SFR was altered by TD0642.

### **FCS\_COP.1(c)/L1 Cryptographic Operation (Hash Algorithm)**

FCS\_COP.1.1(c) Refinement The TSF shall perform cryptographic hashing services in accordance with **[SHA-1]** that meet the following: **[ISO/IEC 10118-3:2004]**.

### **FCS\_COP.1(c)/L2 Cryptographic Operation (Hash Algorithm)**

FCS\_COP.1.1(c) Refinement The TSF shall perform cryptographic hashing services in accordance with **[SHA-256, SHA-384, SHA-512]** that meet the following: **[ISO/IEC 10118-3:2004]**.

### **FCS\_COP.1(d) Cryptographic Operation (AES Data Encryption/Decryption)**

FCS\_COP.1.1(d) The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [CBC] mode** and

cryptographic key sizes **[256 bits]** that meet the following: **AES as specified in ISO/IEC 18033-3, [CBC as specified in ISO/IEC 10116].**

#### **FCS\_COP.1(f) Cryptographic Operation (Key Encryption)**

FCS\_COP.1.1(f) Refinement The TSF shall perform **key encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [CBC mode]** and cryptographic key sizes **[256 bits]** that meet the following: **AES as specified in ISO /IEC 18033-3, [CBC as specified in ISO/IEC 10116].**

#### **FCS\_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)**

FCS\_COP.1.1(g) Refinement The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-[SHA-256, SHA-384, SHA-512]**, key size **[64 (when using SHA-256), 128 (when using SHA-384 or SHA-512)]**, and message digest sizes **[256, 384, 512]** bits that meet the following: **FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, "Secure Hash Standard."**

#### **FCS\_HTTPS\_EXT.1 Extended: HTTPS selected**

FCS\_HTTPS\_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS\_HTTPS\_EXT.1.2 The TSF shall implement the HTTPS protocol using TLS as specified in FCS\_TLS\_EXT.1.

#### **FCS\_IPSEC\_EXT.1 Extended: IPsec selected**

FCS\_IPSEC\_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS\_IPSEC\_EXT.1.2 The TSF shall implement [transport mode, tunnel mode].

FCS\_IPSEC\_EXT.1.3 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS\_IPSEC\_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using [the cryptographic algorithms AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC].

FCS\_IPSEC\_EXT.1.5 The TSF shall implement the protocol: [IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, [no other RFCs for extended sequence numbers], and [RFC 4868 for hash functions];].

FCS\_IPSEC\_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv1] protocol uses the cryptographic algorithms [no other algorithm].

FCS\_IPSEC\_EXT.1.7 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS\_IPSEC\_EXT.1.8 The TSF shall ensure that [IKEv1 SA lifetimes can be established based on length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs]

FCS\_IPSEC\_EXT.1.9 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [no other DH groups].

FCS\_IPSEC\_EXT.1.10 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [RSA] algorithm and Pre-shared Keys.

Application Note: This SFR is altered by TD0157

### **FCS\_KYC\_EXT.1 Extended: Key Chaining**

FCS\_KYC\_EXT.1.1 The TSF shall maintain a key chain of: [intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s): [key encryption as specified in FCS\_COP.1(f)] while maintaining an effective strength of [256 bits].

### **FCS\_RBG\_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)**

FCS\_RBG\_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [NIST SP 800-90A] using [Hash\_DRBG (**any** SHA-256)].

FCS\_RBG\_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [one(1)] hardware-based noise source(s) with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

### **FCS\_TLS\_EXT.1 Extended: TLS selected**

FCS\_TLS\_EXT.1.1 The TSF shall implement one or more of the following protocols [TLS 1.2 (RFC 5246)] supporting the following cipher suites:

- [
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
  - TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
  - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
  - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
  - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
  - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384]

Application Note: This SFR is altered by TD0474

### 5.3.3 User Data Protection (FDP)

#### FDP\_ACC.1 Subset access control

FDP\_ACC.1.1 Refinement The TSF shall enforce the **User Data Access Control SFP** on subjects, objects, and operations among subjects and objects specified in ~~Table 2 and Table 3~~ **Table 19 and Table 20**.

#### FDP\_ACF.1 Security attribute based access control

FDP\_ACF.1.1 Refinement The TSF shall enforce the **User Data Access Control SFP** to objects based on the following: subjects, objects, and attributes specified in ~~Table 2 and Table 3~~ **Table 19 and Table 20**.

FDP\_ACF.1.2 Refinement: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in ~~Table 2 and Table 3~~ Table 19 and Table 20**.

FDP\_ACF.1.3 Refinement: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *[no additional rules]*.

FDP\_ACF.1.4 Refinement: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *[no additional rules]*.

**Table 19: D.USER.DOC Access Control SFP**

|                     |                 | "Create e"                      | "Read"                                    | "Modify"               | "Delete"               |
|---------------------|-----------------|---------------------------------|---|------------------------|------------------------|
| <b>Print (+PRT)</b> | Operation:      | Submit a document to be printed | View image or Release printed output      | Modify stored document | Delete stored document |
|                     | Job owner       | Allowed (note 1)                | View: allowed<br>Release: allowed         | No function            | Allowed                |
|                     | U.ADMIN         | No function                     | View: no function<br>Release: no function | No function            | Allowed                |
|                     | U.NORMAL        | Allowed                         | Denied                                    | Denied                 | Denied                 |
|                     | Unauthenticated | (condition 1)                   | Denied                                    | Denied                 | Denied                 |

|                           |                 | "Create e"                         | "Read"  | "Modify"             | "Delete"             |
|---------------------------|-----------------|------------------------------------|---|----------------------|----------------------|
| <b>Scan (+SCN)</b>        | Operation:      | Submit a document for scanning     | View scanned image                                | Modify stored image  | Delete stored image  |
|                           | Job owner       | Allowed (note 2)                   | Allowed   | No function          | Allowed              |
|                           | U.ADMIN         | No function                        | No function                                       | No function          | Allowed              |
|                           | U.NORMAL        | Allowed                            | Denied  | Denied (No function) | Denied (No function) |
|                           | Unauthenticated | Denied                             | Denied  | Denied (No function) | Denied (No function) |
| <b>Copy (+CPY)</b>        | Operation:      | Submit a document for copying      | View scanned image or Release printed copy output | Modify stored image  | Delete stored image  |
|                           | Job owner       | Allowed (note 2)                   | View: no function<br>Release: no function         | No function          | No Function          |
|                           | U.ADMIN         | No function                        | View: no function<br>Release: no function         | No function          | No Function          |
|                           | U.NORMAL        | Allowed                            | Denied  | Denied (No function) | Denied (No function) |
|                           | Unauthenticated | Denied                             | Denied  | Denied (No function) | Denied (No function) |
| <b>Fax send (+FAXOUT)</b> | Operation:      | Submit a document to send as a fax | View scanned image                                | Modify stored image  | Delete stored image  |
|                           | Job owner       | Allowed (note 2)                   | Allowed   | No function          | Allowed              |
|                           | U.ADMIN         | No function                        | No function                                       | No function          | Allowed              |
|                           | U.NORMAL        | Allowed                            | Denied  | Denied (No function) | Denied (No function) |

|                            |                 | "Create e"                 | "Read"                                       | "Modify"                     | "Delete"                     |
|----------------------------|-----------------|----------------------------|--|------------------------------|------------------------------|
|                            | Unauthenticated | Denied                     | Denied                                       | Denied (No function)         | Denied (No function)         |
| Fax receive (+FAXIN)       | Operation:      | Receive a fax and store it | View fax image or Release printed fax output | Modify image of received fax | Delete image of received fax |
|                            | Fax owner       | Allowed (note 3)           | View: allowed<br>Release: allowed            | No function                  | Allowed                      |
|                            | U.ADMIN         | Allowed (note 4)           | View: no function<br>Release: no function    | No function                  | No function                  |
|                            | U.NORMAL        | Allowed (note 4)           | Denied                                       | Denied                       | Denied                       |
|                            | Unauthenticated | Allowed                    | Denied                                       | Denied                       | Denied                       |
| Storage / retrieval (+DSR) | Operation:      | Store document             | Retrieve stored document                     | Modify stored document       | Delete stored document       |
|                            | Job owner       | Allowed (note 1)           | Allowed                                      | Denied                       | Allowed                      |
|                            | U.ADMIN         | No function                | Denied                                       | Denied                       | Allowed                      |
|                            | U.NORMAL        | Allowed                    | Denied                                       | Denied                       | Denied                       |
|                            | Unauthenticated | (condition 1)              | Denied                                       | Denied                       | Denied                       |

**Table 20: D.USER.JOB Access Control SFP**

|              |            | "Create"         | "Read"                 | "Modify"         | "Delete"         |
|--------------|------------|------------------|------------------------|------------------|------------------|
| Print (+PRT) | Operation: | Create print job | View print queue / log | Modify print job | Cancel print job |
|              | Job owner  | (note 1)         | Allowed                | No function      | Allowed          |
|              | U.ADMIN    | No function      | Allowed                | No function      | Allowed          |

|                         |                 | "Create"               | "Read"                        | "Modify"               | "Delete"               |
|-------------------------|-----------------|------------------------|-------------------------------|------------------------|------------------------|
|                         | U.NORMAL        | Allowed                | Allowed                       | Denied                 | Denied                 |
|                         | Unauthenticated | Denied                 | Allowed                       | Denied                 | Denied                 |
| Scan<br>(+SCN)          | Operation:      | Create scan job        | View scan status / log        | Modify scan job        | Cancel scan job        |
|                         | Job owner       | (note 2)               | Allowed                       | No function            | Allowed                |
|                         | U.ADMIN         | No function            | Allowed                       | No function            | Allowed                |
|                         | U.NORMAL        | Allowed                | Allowed                       | Denied                 | Denied                 |
|                         | Unauthenticated | Denied                 | Denied                        | Denied                 | Denied                 |
| Copy<br>(+CPY)          | Operation:      | Create copy job        | View copy status / log        | Modify copy job        | Cancel copy job        |
|                         | Job owner       | (note 2)               | Allowed                       | No function            | Allowed                |
|                         | U.ADMIN         | No function            | Allowed                       | No function            | Denied                 |
|                         | U.NORMAL        | Allowed                | Denied                        | Denied                 | Denied                 |
|                         | Unauthenticated | Denied                 | Denied                        | Denied                 | Denied                 |
| Fax send<br>(+FAXOUT)   | Operation:      | Create fax send job    | View fax job queue / log      | Modify fax send job    | Cancel fax send job    |
|                         | Job owner       | (note 2)               | Allowed                       | Allowed                | no function            |
|                         | U.ADMIN         | No function            | Allowed                       | No function            | no function            |
|                         | U.NORMAL        | Allowed                | Allowed                       | Denied                 | Denied                 |
|                         | Unauthenticated | Denied                 | Denied                        | Denied                 | Denied                 |
| Fax receive<br>(+FAXIN) | Operation:      | Create fax receive job | View fax receive status / log | Modify fax receive job | Cancel fax receive job |
|                         | Fax owner       | (note 3)               | Allowed                       | No function            | Allowed                |
|                         | U.ADMIN         | (note 4)               | Allowed                       | No function            | Allowed                |
|                         | U.NORMAL        | (note 4)               | Allowed                       | Denied                 | Denied                 |



|                            |                 | "Create"                       | "Read"                       | "Modify"                       | "Delete"                       |
|----------------------------|-----------------|--------------------------------|------------------------------|--------------------------------|--------------------------------|
|                            | Unauthenticated | Allowed                        | Denied                       | Denied                         | Denied                         |
| Storage / retrieval (+DSR) | Operation:      | Create storage / retrieval job | View storage / retrieval log | Modify storage / retrieval job | Cancel storage / retrieval job |
|                            | Job owner       | (note 1)                       | Allowed                      | No function                    | No function                    |
|                            | U.ADMIN         | No function                    | Allowed                      | No function                    | No function                    |
|                            | U.NORMAL        | Allowed                        | Allowed                      | Denied                         | Denied                         |
|                            | Unauthenticated | (condition 1)                  | Denied                       | Denied                         | Denied                         |

Application notes:

Condition 1: Jobs submitted by unauthenticated users must contain a credential that the TOE can use to identify the Job Owner.

See also the following Notes that are referenced in **Table 2 and Table 3 Table 19 and Table 20.**

- Note 1: Job Owner is identified by a credential or assigned to an authorized User as part of the process of submitting a print or storage Job.
- Note 2: Job Owner is assigned to an authorized User as part of the process of initiating a scan, copy, fax send, or retrieval Job.
- Note 3: Job Owner of received faxes is assigned by default or configuration. Minimally, ownership of received faxes is assigned to a specific user or U.ADMIN role.
- Note 4: PSTN faxes are received from outside of the TOE, they are not initiated by Users of the TOE.
- Note 5: Viewing is not permitted and releasing the document is permitted.
- Note 6: Secure Fax must be enabled.

**FDP\_DSK\_EXT.1 Extended: Protection of Data on Disk**

FDP\_DSK\_EXT.1.1 The TSF shall [perform encryption in accordance with FCS\_COP.1(d)] such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.

FDP\_DSK\_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

**FDP\_FXS\_EXT.1 Extended: Fax separation**

FDP\_FXS\_EXT.1.1 The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.

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

FDP\_RIP.1.1(a) Refinement The TSF shall ensure that any previous information content of a resource is made unavailable **by overwriting data** upon the **deallocation of the resource from** the following objects: **D.USER.DOC**.

### 5.3.4 Identification and Authentication (FIA)

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

FIA\_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [ 1 to 5]] unsuccessful authentication attempts occur related to [

- *User authentication using the Operation Panel*
- *User authentication using WIM from the client computer*
- *User authentication when printing from the client computer*
- *User authentication when using LAN Fax from the client computer*].

FIA\_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock the user account for an administrator configurable time period*].

Application Note: This SFR applies only to internal identification and authentication.

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

FIA\_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*Login User Name, User Role, Available Functions List*]

#### FIA\_PMG\_EXT.1 Extended: Password Management

FIA\_PMG\_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

- a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [!"#\$%&'()\*+,-./:;<=>?@[\]^\_`{|}~];
- b) Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

#### FIA\_PSK\_EXT.1 Extended: Pre-Shared Key Composition

FIA\_PSK\_EXT.1.1 The TSF shall be able to use pre-shared keys for IPsec.

FIA\_PSK\_EXT.1.2 The TSF shall be able to accept text-based pre-shared keys that are:

- 22 characters in length and [1-32 characters];

- composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “\*”, “(”, and “)”).

FIA\_PSK\_EXT.1.3 The TSF shall condition the text-based pre-shared keys by using [SHA-256] and be able to [use no other pre-shared keys].

### **FIA\_UAU.1            Timing of authentication**

FIA\_UAU.1.1 Refinement        The TSF shall allow [*the viewing of the list of user jobs, WIM Help, system status, counter and information of inquiries, and creation of fax reception and print jobs*] on behalf of the user to be performed before the user is authenticated.

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

### **FIA\_UAU.7            Protected Authentication Feedback**

FIA\_UAU.7.1                    The TSF shall provide only [*displaying dummy characters as authentication feedback on the Operation Panel and through WIM*] to the user while the authentication is in progress.

### **FIA\_UID.1            Timing of identification**

FIA\_UID.1.1 Refinement        The TSF shall allow [*the viewing of the list of user jobs, WIM Help, system status, counter and information of inquiries, creation of fax reception jobs, and creation of print jobs*] on behalf of the user to be performed before the user is identified.

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

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

FIA\_USB.1.1                    The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*username, available function list, and user role*].

FIA\_USB.1.2                    The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*an Available functions list is associated with the user after the user is authenticated, and the set of available functions does not change during the user session.*]

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: [*none*].

## **5.3.5        Security Management (FMT)**

### **FMT\_MOF.1            Management of security functions behavior**

FMT\_MOF.1.1 Refinement The TSF shall restrict the ability to [determine the behaviour of, disable, enable, modify the behaviour of] the functions [*listed in Table 21*] to **U.ADMIN**.

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

FMT\_MSA.1.1 Refinement The TSF shall enforce the **User Data Access Control SFP** to restrict the ability to [query, modify] the security attributes [*Available function list*] to [*U.ADMIN*].

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

FMT\_MSA.3.1 Refinement The TSF shall enforce the **User Data Access Control SFP** to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT\_MSA.3.2 Refinement The TSF shall allow the **U.ADMIN** to specify alternative initial values to override the default values when an object or information is created.

**FMT\_MTD.1 Management of TSF data**

FMT\_MTD.1.1 Refinement The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 21.**

**Table 21: Management of TSF Data**

| Data  | Operation             | Interfaces           | Authorized Role(s)            |
|---|-----------------------|----------------------|-------------------------------|
| <i>TSF Data owned by U.NORMAL or associated with documents or jobs owned by U.NORMAL.</i>   |                       |                      |                               |
| <i>Login password for authenticated user</i>  | <u>Modify</u>         | Operation Panel, WIM | The Owing U.NORMAL or U.ADMIN |
| <i>TSF Data not owned by a U.NORMAL</i>   |                       |                      |                               |
| <i>Audit Logs</i>   | <u>Delete, Export</u> | WIM                  | U.ADMIN                       |
| <i>Login passwords of U.ADMIN user</i>  | <u>Modify</u>         | Operation Panel, WIM | U.ADMIN                       |
| <i>Username, user role, available function list or access permissions of U.NORMAL Users</i> | <u>Modify</u>         | Operation Panel, WIM | U.ADMIN                       |
| <i>HDD Cryptographic Key</i>  | <u>Create, Delete</u> | Operation Panel      | U.ADMIN                       |
| <i>Software, firmware, and related configuration data</i>                                   |                       |                      |                               |

| Data   | Operation                     | Interfaces           | Authorized Role(s) |
|--|-------------------------------|----------------------|--------------------|
| <i>Audit Transfer Settings</i>                               | <u>Modify</u>                 | WIM                  | U.ADMIN            |
| <i>Date &amp; Time Settings</i>                              | <u>Modify</u>                 | Operation Panel, WIM | U.ADMIN            |
| <i>Password Length and Password complexity settings</i>      | <u>Modify</u>                 | Operation Panel, WIM | U.ADMIN            |
| <i>Operation Panel Auto logout settings</i>                  | <u>Modify</u>                 | Operation Panel      | U.ADMIN            |
| <i>WIM Auto logout settings</i>                              | <u>Modify</u>                 | WIM                  | U.ADMIN            |
| <i>PSTN Fax-Line Separation - Stored Reception File User</i> | <u>Modify</u>                 | Operation Panel      | U.ADMIN            |
| <i>Device Certificate</i>                                    | <u>Create, Modify, Delete</u> | Operation Panel, WIM | U.ADMIN            |
| <i>TOE Software updates</i>                                  | <u>Modify</u>                 | WIM                  | U.ADMIN            |
| <i>Network settings for trusted communication</i>            | <u>Modify</u>                 | Operation Panel, WIM | U.ADMIN            |

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

FMT\_SMF.1.1 Refinement The TSF shall be capable of performing the following management functions: [*management functions listed in Table 22*]

**Table 22: Management Functions**

| Management Functions   | Operation                     | Interface(s)         |
|--|-------------------------------|----------------------|
| Manage user accounts (users, roles, privileges and available functions list) | <i>Create, modify, delete</i> | Operation Panel, WIM |
| Manage the document user list for stored documents                           | <i>Create, modify</i>         | Operation Panel, WIM |
| Configure audit transfer settings  | <i>Modify</i>                 | WIM                  |
| Manage audit logs  | <i>Delete, export</i>         | Operation Panel, WIM |
| Manage Audit Functions   | <i>Enable,</i>                | Operation Panel, WIM |

| Management Functions  | Operation                     | Interface(s)         |
|---|-------------------------------|----------------------|
|   | <i>Disable</i>                |                      |
| Manage time and date settings   | <i>Modify</i>                 | Operation Panel, WIM |
| Configure minimum password length   | <i>Modify</i>                 | Operation Panel, WIM |
| Configure Password complexity settings  | <i>Modify</i>                 | Operation Panel, WIM |
| Configure Operation Panel Auto Logout Time  | <i>Modify</i>                 | Operation Panel, WIM |
| Configure WIM Auto Logout Time  | <i>Modify</i>                 | WIM                  |
| Configure number of authentication failure before account lockout   | <i>Modify</i>                 | WIM                  |
| Configure account release timer settings  | <i>Modify</i>                 | WIM                  |
| Configure PSTN Fax-Line Separation Stored Reception File User   | <i>Modify</i>                 | Operation Panel, WIM |
| Configure image overwrite   | <i>Modify</i>                 | Operation Panel      |
| Configure network settings for trusted communications (specify IP addresses and port to connect to the TOE) | <i>Modify</i>                 | Operation Panel, WIM |
| Manage HDD Cryptographic key  | <i>Create Delete</i>          | Operation Panel      |
| Manage Device Certificates  | <i>Create, modify, delete</i> | Operation Panel, WIM |
| Manage TOE Trusted Update   | <i>Query, Modify</i>          | WIM                  |
| Configure IPSec   | <i>Modify</i>                 | WIM                  |
| Configure SMTP over IPSec   | <i>Modify</i>                 | WIM                  |
| Configure NTP   | <i>Modify</i>                 | WIM                  |

### FMT\_SMR.1 Security roles

FMT\_SMR.1.1 Refinement The TSF shall maintain the roles **U.ADMIN, U.NORMAL**.

FMT\_SMR.1.2 The TSF shall be able to associate users with roles.

### 5.3.6 Protection of the TSF (FPT)

#### FPT\_KYP\_EXT.1 Extended: Protection of Key and Key Material

FPT\_KYP\_EXT.1.1 The TSF shall not store plaintext keys that are part of the keychain specified by FCS\_KYC\_EXT.1 in **any Field-Replaceable Nonvolatile Storage Device**.

#### FPT\_SKP\_EXT.1 Extended: Protection of TSF Data

FPT\_SKP\_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

#### FPT\_STM.1 Reliable Time Stamps

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

#### FPT\_TST\_EXT.1 Extended: TSF testing

FPT\_TST\_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

#### FPT\_TUD\_EXT.1 Extended: Trusted update

FPT\_TUD\_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT\_TUD\_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT\_TUD\_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [no other functions] prior to installing those updates.

### 5.3.7 TOE Access (FTA)

#### FTA\_SSL.3 TSF-initiated Termination

FTA\_SSL.3.1 The TSF shall terminate interactive session after a *[lapse of Operation Panel auto logout time, lapse of WIM auto logout time, completion of document data reception from the printer driver, and completion of document data reception from the fax driver]*.

### 5.3.8 Trusted path/channels (FTP)

#### FTP\_ITC.1/TLS Inter-TSF trusted channel

FTP\_ITC.1.1/TLS Refinement The TSF shall use **[TLS]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: [Syslog, LDAP and SMTP]**

that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

- FTP\_ITC.1.2/TLS Refinement The TSF shall permit **the TSF, or the authorized IT entities**, to initiate communication via the trusted channel.
- FTP\_ITC.1.3/TLS Refinement The TSF shall initiate communication via the trusted channel for [*communication via the LAN of document data, function data, protected data, and confidential data*].
- FTP\_ITC.1/IPSEC Inter-TSF trusted channel**
- FTP\_ITC.1.1/IPSEC Refinement The TSF shall use **[IPsec]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: [authentication server, [FTP, NTP, Syslog, and SMTP]]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.
- FTP\_ITC.1.2/IPSEC Refinement The TSF shall permit **the TSF, or the authorized IT entities**, to initiate communication via the trusted channel.
- FTP\_ITC.1.3/IPSEC Refinement The TSF shall initiate communication via the trusted channel for [*communication via the LAN of document data, function data, protected data, and confidential data*].

**FTP\_TRP.1(a) Trusted Path (for Administrators)**

- FTP\_TRP.1.1(a) Refinement The TSF shall use **[TLS/HTTPS]** to provide a **trusted** communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.
- FTP\_TRP.1.2(a) Refinement The TSF shall permit **remote administrators** to initiate communication via the trusted path.
- FTP\_TRP.1.3(a) Refinement The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions**.

**FTP\_TRP.1(b) Trusted Path (for Non-administrators)**

- FTP\_TRP.1.1(b) Refinement The TSF shall use **[TLS/HTTPS]** to provide a **trusted** communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.



FTP\_TRP.1.2(b) Refinement The TSF shall permit [the TSF, remote users] to initiate communication via the trusted path.

FTP\_TRP.1.3(b) Refinement The TSF shall require the use of the trusted path for **initial user authentication and all remote actions.**

## 5.4 Assurance Requirements

35 The TOE security assurance requirements are summarized in Table 23.

**Table 23: TOE Security Assurance Requirements**

| Assurance Class            | Components | Description   |
|----------------------------|------------|---|
| Security Target Evaluation | ASE_CCL.1  | Conformance Claims                                  |
|                            | ASE_ECD.1  | Extended Components Definition                      |
|                            | ASE_INT.1  | ST Introduction                                     |
|                            | ASE_OBJ.1  | Security Objectives for the operational environment |
|                            | ASE_REQ.1  | Stated Security Requirements                        |
|                            | ASE_SPD.1  | Security Problem Definition                         |
|                            | ASE_TSS.1  | TOE Summary Specification                           |
| Development                | ADV_FSP.1  | Basic Functional Specification                      |
| Guidance Documents         | AGD_OPE.1  | Operational User Guidance                           |
|                            | AGD_PRE.1  | Preparative procedures                              |
| Life Cycle Support         | ALC_CMC.1  | Labelling of the TOE                                |
|                            | ALC_CMS.1  | TOE CM Coverage                                     |
| Tests                      | ATE_IND.1  | Independent Testing - conformance                   |
| Vulnerability Assessment   | AVA_VAN.1  | Vulnerability survey                                |

## 6 TOE Summary Specification

36 The following describes how the TOE fulfils each SFR included in section 5.3.

### 6.1 Security Audit

#### 6.1.1 FAU\_GEN.1 & FAU\_GEN.2

37 The TOE records an audit log of events listed in Table 24. Audit log entries record the date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. Additionally, Job Completion events record the type of job, and Failure to Establish Session events record the reason for such failure.

**Table 24: List of Audit Events**

| Auditable event requirements                                       | Auditable events satisfied                                  |
|--|---|
| Start-up and shutdown of the audit functions                       | Start-up of the Audit Function                              |
|  | Shutdown of the Audit Function                              |
| Job completion   | Printing via networks                                       |
|  | LAN Fax via networks  |
|  | Scanning documents  |
|  | Copying documents   |
|  | Receiving incoming faxes                                    |
|  | Creating document data (storing)                            |
|  | Reading document data (print, download, fax transmission)   |
|  | Deleting document data                                      |
| Unsuccessful User authentication, Unsuccessful User identification | Failure of login operations                                 |
| Use of management functions  | Use of functions identified in FMT_SMF.1                    |
| Modification to the group of Users that are part of a role         | Modification of MFP Administrator roles                     |
| Changes to the time  | Date settings (year/month/day), time settings (hour/minute) |
| Failure to establish session                                       | Failure of communication with the audit server              |

| Auditable event requirements | Auditable events satisfied                              |
|------------------------------|---|
|                              | Failure of communication with the authentication server |
|                              | Failure of communication with the FTP server            |
|                              | Failure of communication with the NTP server            |
|                              | Failure of communication with print driver              |
|                              | Failure of communication with fax driver                |
|                              | Failure of communication with WIM                       |

**6.1.2 FAU\_STG.1, FAU\_STG\_EXT.1, FAU\_STG.4, FAU\_SAR.1, FAU\_SAR.2, FTP\_ITC.1/TLS, and FTP\_ITC.1/IPSEC**

38 The TOE stores audit log data in a dedicated storage area of the HDD. Audit records are buffered in that storage area before transfer to a configured remote syslog server over a configured TLS or IPsec trusted channel.

39 Authorized administrators use the WIM to review the audit trail and to initiate transfer of audit records. The TOE prevents unauthorized access to the audit records by ensuring that the options to manage the audit function and the audit records are not included in the lists of available functions visible to the U.NORMAL users.

40 The TOE audit trail comprises three types of audit logs: Job logs, Access logs, and Ecology logs. By default, the job and ecology logs will each hold a maximum of 4,000 records; the access log can have a maximum of 12,000 records. When a maximum number of records is reached, the oldest records are overwritten based on the following criteria:

- a) When syslog audit transfers are working, the oldest records which have been transferred to the syslog server are overwritten first.
- b) If none of the logs have been transferred to the audit server, the oldest records are overwritten first.

**6.2 Identification and Authentication**

**6.2.1 FIA\_UAU.1, FIA\_UID.1, FIA\_UAU.7, FIA\_ATD.1 & FIA\_USB.1**

41 For each individual user, the TOE maintains the user attributes: login username, password, user role and available functions list regardless of the authentication method for the user account. Users login to the TOE by entering their username/password credentials on the Operation Panel, the WIM login screen, or through a client's print driver or fax driver that has been configured to submit user credentials.

42 When users enter their passwords on the Operation Panel or the WIM login, the TOE displays a sequence of dummy characters whose length is the same as that of the entered password.

43 All users accessing the TOE user interfaces are identified and authenticated before they are allowed access. Only the following functions are accessible before the user is authenticated:

- a) Viewing user job lists, WIM Help, system status, the counter and information of inquiries.
- b) Creation of fax reception jobs.
- c) Creation of print jobs

44 The TOE authenticates users by checking the entered username/passwords credentials against the local user database or against an external authentication service (LDAP).

45 An available functions list that identifies the basic hardcopy functions a user is permitted to perform is associated with each Normal User. After successful login, users are authorized to perform functions according to their assigned user role (Normal User, MFP Administrator, or MFP Supervisor). If login fails, the user is denied access to all functions that require user authentication.

### 6.2.2 FIA\_PMG\_EXT.1

46 For authentication within the TOE, login passwords for users can be registered only if these passwords meet the conditions specified by the selections in FIA\_PMG\_EXT.1.

### 6.2.3 FIA\_AFL.1 & FTA\_SSL.3

47 The TOE counts consecutive login failures for a given login name and will lock out that user after an administrator-configured number of authentication failures attempts have been reached. For the U.NORMAL users, the account lockout is released when the configured lockout time has elapsed or by direct release operation performed by the MFP administrator. For the U.ADMIN users, the account lockout is released when the configured lockout time has elapsed, or by direct release operation performed by the MFP Administrator or MFP Supervisor, or by elapse of a given time after the TOE restarts.

48 The TOE can terminate user sessions at the various interfaces as follow:

- a) **Operation Panel:** the user is logged out of the TOE when inactivity reaches the Operation Panel auto logout time (settable from 10 to 999 seconds).
- b) **WIM:** the user is logged out of the TOE when inactivity reaches the WIM auto logout time (settable from 3 to 60 minutes).
- c) **Printer driver:** the user is logged out of the TOE immediately after receiving the print data from the printer driver.
- d) **Fax driver:** the user is logged out of the TOE immediately after receiving the transmission information from the fax driver.

## 6.3 Access Control

### 6.3.1 FDP\_ACC.1 & FDP\_ACF.1

49 The TOE controls user operations for document data and user jobs as specified in Table 19 and Table 20.

**6.3.1.1 Access control rule on document data**

- 50 The TOE provides users with the ability to perform operations on document data that are stored in the TOE.
- 51 Normal Users are permitted to operate on document data if the ID of the user corresponds to the Document User List for that document (i.e., the user is the "Job Owner"). A Normal User is not permitted to operate on document data for which it is not the Job Owner.
- 52 A Normal User who is a Job Owner may print, download to client computers, send by fax, send by e-mail as attachments, and delete stored documents, using the Operation Panel or a web browser.
- 53 The TOE allows only the Job Owner to view and delete the document data handled as a user job while Copy Function, Printer Function, Scanner Function, Fax Function, or Document Server Function is being used.
- 54 While no interface to change job owners is provided, an interface to cancel user jobs is provided. If a user job is cancelled, any document the cancelled job operates will be deleted.

**Table 25: Stored Documents Access Control Rules for Normal Users**

| Function        | User interface  | Type of document | Operations permitted for authorized users  |
|-----------------|-----------------|------------------|--|
| Printer         | Operation Panel | +PRT             | Print<br>Delete  |
| Printer         | Web browser     | +PRT             | Delete   |
| Scanner         | Operation Panel | +SCN             | E-mail transmission  |
| Fax             | Operation Panel | +FAXIN           | Print<br>Delete  |
| Fax             | Web browser     | +FAXIN           | Download<br>Delete<br>(Operations above are permitted only if Normal Users are authorized to use Document Server Function) |
| Document Server | Operation Panel | +DSR             | Print<br>Delete  |
| Document Server | Operation Panel | +FAXOUT          | Print<br>Delete  |
| Document Server | Web browser     | +DSR             | Delete   |
| Document Server | Web browser     | +FAXOUT          | Fax transmission<br>Download   |

| Function | User interface | Type of document | Operations permitted for authorized users   |
|----------|----------------|------------------|---|
|          |                |                  | Delete<br>(Fax transmission is permitted for Normal Users who are authorized to use Fax Function) |

55 MFP Administrators are not permitted to print, download, or send stored documents. MFP Administrators may delete stored documents, using the Operation Panel, web browser, or indirectly by cancelling a job.

56 The MFP Supervisor is not permitted to perform any document operations.

**6.3.1.2 Access control rule on user jobs**

57 The TOE displays on the Operation Panel a menu to cancel a user job only if the user who logs in from the Operation Panel is a Job Owner or MFP Administrator and a cancellation of a user job is attempted by the Job Owner or an MFP Administrator. Other users are not allowed to operate user jobs.

58 When a user job is cancelled, any documents operated by the cancelled job will be deleted. However, if the document data operated by the cancelled user job is a stored document, the data will not be deleted and remain stored in the TOE.

**6.4 Cryptographic Operations**

**6.4.1 FCS\_CKM.1 (a), FCS\_CKM.1(b)/DIM, FCS\_CKM.1(b)/DAR, FCS\_RBG\_EXT.1.**

59 The TOE implements random-bit generation services using a software based DRBG that has been seeded with at least 256-bits of entropy from a third-party hardware-based TRNG and DRBG.

**Table 26: Random Number Sources**

| RNG           | Method            | Standard      | RNG           |
|---------------|-------------------|---------------|---------------|
| Hardware TRNG | True RNG + DRBG   | AIS31 Class 2 | Hardware TRNG |
| Software DRBG | Hash_DRBG_SH A256 | SP 800-90A    | Software DRBG |

60 The TOE generates cryptographic keys upon initial start-up, as a result of administrative actions and during communication sessions. Using a Hash-DRBG, the TOE generates a KEK, HDD Key, NVRAM Key and DevCert Key, which it uses for data encryption; TLS session keys, IPsec IKE key and ESP key which it uses for trusted communications.

For all encryption operations the TOE uses AES 256 in CBC mode and the following cryptographic keys:

- a) FFC DH Groups 14 (2048-bit MODP)
- b) ECDHE P-256
- c) RSA 2048

d) 128-bit and 256-bit symmetric keys

61 Additional details about key creation, the TRNG, and the DRBG, are provided in the Key Management Description and Entropy Description documents.

**6.4.2 FPT\_SKP\_EXT.1, FCS\_CKM.4 and FCS\_CKM\_EXT.4**

62 All pre-shared keys, symmetric keys, and private keys are protected in storage and are not accessible to any user through TOE interfaces. A root encryption key is securely stored in IKey (a Trusted Platform Module). No other plaintext keys are stored in non-volatile storage. The root encryption key is used to decrypt a key encryption key which is used to decrypt symmetric keys for encrypted storage and the Device Certificate. The Ipsec PSK is stored in an encrypted partition of NVRAM. Key destruction is described in the Key Management Description.

63 The TOE destroys cryptographic keys and key materials when no longer needed. TLS and Ipsec session keys are no longer needed at the end of a communication session. The REK, KEK, NVRAM Key, and DevCert Key are always needed and are never destroyed in the evaluated configuration. HDD encryption is always enabled in the evaluated configuration, so the HDD key is always needed. Cryptographic keys and key materials stored by the TOE can be destroyed by overwriting the key with the value of a new key; the HDD key can be logically deleted should HDD encryption be disabled. Key destruction is further described in the separate proprietary Key Management Document (KMD).

**6.5 Stored Data Encryption**

**6.5.1 FCS\_KYC\_EXT.1, FPT\_KYP\_EXT.1, and FCS\_COP.1(f)**

64 The TOE encrypts data on the HDD and in NVRAM. The keychain for encrypting field-replaceable non-volatile storage devices begins with a common Root Encryption Key (REK). The plaintext REK is stored in a hardware security module, IKey.

65 The REK is used to encrypt and decrypt a Key Encryption Key (KEK). The KEK is used to encrypt and decrypt Device Encryption Keys (DEKs) for the HDD and NVRAM. All such operations use 256-bit AES keys to protect 256-bit AES data encryption on the target devices.

**Table 27: Keychain encryption**

| Key                       | En/decrypts                         | Algorithm | Length | SFR          |
|---------------------------|-------------------------------------|-----------|--------|--------------|
| Root Encryption Key (REK) | Key Encryption Key                  | AES CBC   | 256    | FCS_COP.1(f) |
| Key Encryption Key (KEK)  | HDD Key<br>NVRAM Key<br>DevCert Key | AES CBC   | 256    | FCS_COP.1(f) |

66 Additional details about the keychain and device encryption are provided in the Key Management Description.



## 6.5.2 FDP\_DSK\_EXT.1 and FCS\_COP.1(d)

67 Two field-replaceable non-volatile storage devices employ encryption: the HDD, and NVRAM.

68 All HDD data is encrypted with AES 256 CBC encryption by a hardware component, Ic Ctrl. HDD encryption is enabled and initialized in the evaluated configuration, as described in the guidance documentation.

69 Partition 3 of NVRAM is encrypted software component, LPUX NVRAM Encryption Driver, with AES 256 CBC encryption. NVRAM encryption is initialized during manufacturing and cannot be disabled. Other partitions of NVRAM do not contain confidential User or TSF Data.

70 Keychain, key management, and other details are provided in the Key Management Description.

## 6.6 Protection of the TSF

### 6.6.1 FPT\_STM.1

71 The date (year/month/day) and time (hour/minute/second) the TOE records for the audit log are derived from the system clock of the TOE. The system clock is also used for other time-related functions, including user lockout timing, idle session timeouts, and SA lifetimes.

72 The system clock may be set locally or configured to use a network time server. Only an MFP Administrator can configure the system clock.

## 6.7 Trusted Communications

73 The Trusted Communications Function provides trusted paths for communications between the TOE and remote users as well as a trusted channel for the TOE to communicate with other remote IT entities.

### 6.7.1 FTP\_TRP.1 (a), FTP\_TRP.1 (b), FCS\_HTTPS\_EXT.1, FTP\_ITC.1/TLS and FCS\_TLS\_EXT.1

74 The TOE implements TLS 1.2 to protect communications between the TOE and remote users' client computers (print drivers, fax drivers, and WIM HTTPS sessions). TLS client authentication is not supported. The TOE can also be configured at initial configuration to use TLS to protect communications with a remote Syslog, LDAP or SMTP server.

75 The TOE supports these ciphersuites:

- a) TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- b) TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- c) TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- d) TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- e) TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- f) TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

### 6.7.2 FCS\_COP.1 (a), FCS\_COP.1(b), FCS\_COP.1(c), and FCS\_COP.1(g)

76 The TOE generates a self-signed Device Certificate according to FCS\_CKM.1(a). Administrators may import a Device Certificate that is generated outside of the TOE.

To establish a session key for TLS communications, the TOE employs a Diffie-Hellman-based key establishment scheme conforming to NIST SP 800-56A Section 5.6, and a Hash DRBG. The session key is used to encrypt communications with AES 128 or AES 256 CBC:

**Table 28: TLS/HTTPS Cryptographic Functions**

| Function                 | SFR           | Algorithm        |
|--------------------------|---------------|------------------|
| Key establishment        | FCS_CKM.1(a)  | DSA KeyGen 186-4 |
|                          | FCS_COP.1(b)  | KAS-FFC          |
|                          | FCS_COP.1(c)  | KAS-ECC          |
| Message Authentication   | FCS_COP.1(g)  | HMAC-SHA-256     |
|                          |               | HMAC-SHA-384     |
|                          |               | HMAC-SHA-512     |
| Random number generation | FCS_RBG_EXT.1 | Hash_DRBG_SHA256 |
| Encryption / decryption  | FCS_COP.1(a)  | AES 128 CBC      |
|                          |               | AES 256 CBC      |
|                          |               | AES 128 GCM      |
|                          |               | AES 256 GCM      |

### 6.7.3 FTP\_ITC.1/IPSEC, FCS\_IPSEC\_EXT.1, FIA\_PSK\_EXT.1, and FCS\_COP.1(g)

77 The TOE employs IPsec to protect communications between the TOE and external IT entities in the operational environment. In the evaluated configuration, it is used for communications with LDAP, syslog, NTP, SMTP, and FTP servers.

78 IPsec is operated in transport mode or tunnel mode, as set by the administrator.

79 IPsec supports automatic key exchange or automatic key exchange by IKEv1.

80 In Phase 1, peer authentication supports two types of authentication: pre-shared key authentication and digital certificate authentication.

81 The pre-shared key can be any length from 1 to 32 characters, and is composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "\$", "%", "^", "&", "\*", "(", and ")"). Text-based pre-shared keys of 22 characters is supported. The pre-shared key is configurable with an ASCII text string, and it is conditioned using a SHA-256 hash.

82 An administrator can select whether to use main mode or aggressive mode. In the evaluated configuration, only main mode is used.

83 In IKEv1, supported DH group is 14. The value set by the administrator is used.

- 84 IKEv1 key lifetimes can be set by the administrator, from 300 seconds to 172,800 seconds. In the evaluated configuration, Phase 1 key lifetime is set to 86,400 seconds (24 hours), and Phase 2 lifetime is set to 28,800 seconds (8 hours).
- 85 As an SPD, four individual entries and one default entry of Protect can be set by an administrator. Beginning with the first entry the packet is compared, and if it matches the entry, IPsec communication is performed. If the packet does not match the first entry, subsequent entries are tested until there is a match. If no entries match the packet, the default entry will be compared, and if it does not match, the packet is discarded.
- 86 The TOE supports these cryptographic algorithms:

**Table 29: IPsec Cryptographic Functions**

| Function | SFR           | Algorithm                    |
|----------|---------------|------------------------------|
| IKEv1    | FCS_CKM.1(a)  | RSA 186-4                    |
|          | FCS_COP.1(a)  | AES 128 CBC                  |
|          | FCS_COP.1(b)  | AES 256 CBC                  |
|          | FCS_COP.1(g)  | HMAC-SHA-256                 |
|          | FCS_RBG_EXT.1 | HMAC-SHA-384<br>HMAC-SHA-512 |
| ESP      | FCS_COP.1(a)  | AES-128-CBC                  |
|          | FCS_COP.1(b)  | AES-256-CBC                  |
|          | FCS_COP.1(g)  | HMAC-SHA-256                 |
|          | FCS_RBG_EXT.1 | HMAC-SHA-384<br>HMAC-SHA-512 |

## 6.8 Administrative Roles

- 87 The Security Management Function consists of functions to 1) control operations for TSF data, 2) maintain user roles assigned to Normal Users, MFP Administrator, or MFP Supervisor to operate the Security Management Function, and 3) set appropriate default values to security attributes, all of which accord with user role privileges or user privileges that are assigned to Normal Users, MFP Administrator, or MFP Supervisor.

### 6.8.1 FMT\_SMR.1

- 88 The TOE maintains U.NORMAL and U.ADMIN roles as described in Table 6. U.NORMAL defines the normal or non-admin users of the TOE which are permitted to use the document processing functions of the MFP and access their own data. U.ADMIN defines All TOE administrators w which includes the MFP Administrator and the MFP Supervisor. The MFP Administrator configures the TOE, manages normal users' jobs and normal users' data. The MFP supervisor sets MFP Administrators' passwords. Administrators do not initiate document processing jobs.

### 6.8.2 FMT\_SMF.1, FMT\_MOF.1, and FMT\_MTD.1

89 The TOE provides and restricts the following management functions which can be managed over the Operation Panel or the WIM:

- a) Manage user accounts including create, modify, delete users, user roles, privileges, available function lists.
- b) Manage the document user list for stored documents
- c) Manage the audit functions including enable/disable the audit functions and modifying the audit transfer settings
- d) Query, delete and export the audit logs
- e) Configure time and date settings
- f) Password Management including configuring password composition, password length, and password complexity
- g) Configure auto logout settings on WIM and the Operation Panel
- h) Configure Authentication Failure and Account lockout timer settings
- i) Modify PSTN Fax-Line Separation Stored Reception File User
- j) Configure Image Overwrite
- k) Configure network settings for trusted communications (specify IP addresses and port to connect to the TOE)
- l) Manage HDD cryptographic keys
- m) Manage device certificates including create, delete and modify certificates
- n) Manage TOE trusted update
- o) Configure IPsec
- p) Configure SMTP over IPsec
- q) Configure NTP

90 The TOE restricts modification of TSF functions and TSF data to the authorized administrator roles.

### 6.8.3 FMT\_MSA.1 and FMT\_MSA.3

91 Table 19 and Table 20 list the access control rules enforced by the TOE when users access the document processing functions (print, scan, copy, fax) and individual user jobs. The default behaviour to access the document data is permissive for all authenticated normal users, except for the U.ADMIN user which cannot initiate document processing functions. The TOE maintains username and available function lists data for individual users, unauthenticated users sending document print of document fax to the TOE must be identified before the TOE processes the job.

## 6.9 Trusted Operation

92 The Software Verification Function is to verify the integrity of the executable codes of the MFP Control Software, FCU Control Software and Operation Panel Control Software, and confirm that these codes can be trusted.

**6.9.1 FPT\_TST\_EXT.1, FCS\_COP.1(b), FCS\_COP.1(c)/L1, and FCS\_COP.1(c)/L2**

93 During start-up, the TOE performs a series of integrity tests, that check that the hash on the executable files is correct and that the software has not been changed. The integrity tests check the hash on the software executable listed below:

**Table 30: Start-up Integrity Tests**

| Integrity test           | SFR             | Algorithm |
|--------------------------|-----------------|-----------|
| MFP Control Software     | FCS_COP.1(b)    | RSA 186-4 |
|                          | FCS_COP.1(c)/L2 | SHA-256   |
| Fax Control Unit         | FCS_COP.1(c)/L1 | SHA-1     |
| Operation Panel Software | FCS_COP.1(b)    | SHA-256   |
|                          | FCS_COP.1(c)/L2 |           |

94 If any steps of the integrity tests fail, a Service Call (SC) error code is displayed on the Operator Panel and the TOE becomes unavailable. In such cases, the Administrator must contact a Customer Engineer to service the TOE.

95 When all steps succeed, the TOE becomes operational.

96 Testing that the hash on the TOE software image is correct before the TOE can become operational verifies the integrity and validity of the TOE software; this is sufficient to demonstrate that the TSF is operating correctly.

**6.9.2 FPT\_TUD\_EXT.1, FCS\_COP.1(b), FCS\_COP.1(c)/L1, and FCS\_COP.1(c)/L2**

97 TOE allows only the MFP Administrator to read the version of the MFP Control Software, Operation Panel Control Software, and FCU Control Software. The MFP Administrator can read these versions using the Operation Panel or WIM from the client computer.

98 The MFP Administrator can prepare for installation of updated MFP Control Software, Operation Panel Software, or FCU Control Software, by uploading an installation package from the client computer using WIM. The package contains the TOE Software and a digital signature (DS) that was created using the SERES private key. Digital signatures for trusted updates are generated outside of the TOE, by the manufacturer.

99 For MFP Control or FCU Software, the TOE performs the following verifications before the installing the package:

- a) Identifies the type of software (e.g., MFP Control, Operation Panel, FCU);
- b) Verifies that the software model name matches the TOE;
- c) Creates a SHA256 message digest (MD1) of the software, uses the SERES public key to decrypt DS (MD2), and then verifies that MD1 = MD2.

100 For Operation Panel software, the TOE performs the following verifications before the installing the package:

- a) Identifies the type of software (e.g., MFP Control, Operation Panel, FCU);
- b) Verifies that the software model name matches the TOE;

- c) Creates a SHA256 message digest (MD1) of the index file, uses the SERES public key to decrypt DS (MD2), and then verifies that MD1 = MD2.
  - d) Creates a SHA256 message digest (MD3) of the software image, uses an internal key to decrypt DS (MD4), and then verifies that MD3 = MD4.
- 101 For each Operation Panel application, the TOE performs the following verifications before the installing the package:
- a) Verifies that the application is Ricoh's by checking the certificate contained in the APK.
  - b) Creates a SHA256 message digest (MD1) of the application, uses the public key in the certificate to decrypt DS (MD2), and then verifies that MD1 = MD2.
- 102 The TOE performs the signature verification of the software to be updated using the encryption functions listed below when updating the software.

**Table 31: Signature Verification**

| Integrity test               | SFR             | Algorithm |
|------------------------------|-----------------|-----------|
| MFP Control Software         | FCS_COP.1(b)    | RSA 186-4 |
|                              | FCS_COP.1(c)/L2 | SHA-256   |
| Operation Panel Software     | FCS_COP.1(b)    | RSA 186-4 |
|                              | FCS_COP.1(c)/L2 | SHA-256   |
| Operation Panel Applications | FCS_COP.1(b)    | RSA 186-4 |
|                              | FCS_COP.1(c)/L2 | SHA-256   |

Note: MFP Control Software includes FCU Software when Fax is installed on the TOE

## 6.10 PSTN Fax-Network Separation

- 103 The Fax Line Separation Function permits only fax transmissions as input information from telephone lines so that unauthorized intrusion from telephone lines can be prevented.

### 6.10.1 FDP\_FXS\_EXT.1

- 104 The fax interface use cases are below.
- a) Sending faxes
    - i) The TOE receives documents from client PCs via the LAN, and using the fax interface, transmits them as fax documents via the PSTN line using the ITU-T T.30 protocol.
    - ii) The TOE can transmit stored documents as faxes.
  - b) Receiving faxes
    - i) A remote fax machine establishes a connection to the TOE through the PSTN line using the ITU-T T.30 protocol, through which the TOE receives fax documents.
  - c) Fax-Line Separation

- i) The fax modem accepts connections through the PSTN only if they conform to the ITU-T T.30 protocol.
- ii) Data that is transmitted or received through the PSTN is fax-format, image data.

105 Other than the specified use cases, the TOE allows no other data to be transmitted on the fax line.

## 6.11 Image Overwrite

### 6.11.1 FDP\_RIP.1(a)

106 During the processing of jobs, image data is stored on the HDD. When such data is no longer needed by the user or the TOE, residual data can be overwritten using the Auto Erase Memory function.

107 When enabled, the Auto Erase Memory function automatically overwrites the residual image data after each completion of the following processing jobs:

- a) Copy jobs
- b) Print jobs
- c) Sample Print/Locked Print/Hold Print
- d) Stored Print jobs (after deletion of the job)
- e) Spool printing jobs
- f) LAN-Fax print data
- g) Faxes sent/received using remote machines
- h) Scanned files sent by e-mail
- i) Files sent by Scan to Folder
- j) Documents sent using Web Image Monitor
- k) Documents deleted from the Document Server using the Copier, Printer, Fax or Scanner functions

108 When the Auto Erase Memory function is enabled, such data is actively overwritten with values and repetition selected by the Administrator:

- a) NSA: Temporary data is overwritten twice with random numbers and once with zeros.
- b) DoD: Each item of data is overwritten by a random number, then by its complement, then by another random number, and is then verified.
- c) Random Numbers: Temporary data is overwritten multiple times with random numbers. The number of overwrites can be selected from 1 to 9, default 3.

# 7 Rationale

## 7.1 Conformance Claim Rationale

- 109 The following rationale is presented with regard to the PP conformance claims:
- a) **TOE type.** As identified in section 2.1, the TOE is hardcopy device, consistent with the HCDPP.
  - b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced directly from the HCDPP.
  - c) **Security objectives.** As shown in section 4, the security objectives are reproduced directly from the HCDPP.
  - d) **Security requirements.** As shown in section 4, the security requirements are reproduced directly from the HCDPP. No additional requirements have been specified.

## 7.2 Security Objectives Rationale

110 The following table maps threats, OSPs, and assumptions, to their respective Security Objectives.

**Table 32: Security Objectives Rationale**

| Threat/Policy/Assumptions   | Rationale  |
|---|--|
| <p><b>T.UNAUTHORIZED_ACCESS</b><br/>                     An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE’s interfaces.</p> | <p>O.ACCESS_CONTROL restricts access to User Data in the TOE to authorized Users.</p> <p>O.USER_I&amp;A provides the basis for access control.</p> <p>O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators.</p> |
| <p><b>T.TSF_COMPROMISE</b><br/>                     An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE’s interfaces.</p>  | <p>O.ACCESS_CONTROL restricts access to TSF Data in the TOE to authorized Users.</p> <p>O.USER_I&amp;A provides the basis for access control.</p> <p>O.ADMIN_ROLES restricts the ability to authorize Users and set access controls to authorized Administrators.</p>  |
| <p><b>T.TSF_FAILURE</b><br/>                     A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.</p>  | <p>O.TSF_SELF_TEST prevents the TOE from operating if a malfunction is detected.</p>   |
| <p><b>T.UNAUTHORIZED_UPDATE</b><br/>                     An attacker may cause the installation of unauthorized software on the TOE.</p>  | <p>O.UPDATE_VERIFICATION verifies the authenticity of software updates.</p>  |



| Threat/Policy/Assumptions  | Rationale  |
|--|--|
| <p>T.NET_COMPROMISE</p> <p>An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.</p>   | <p>O.COMMS_PROTECTION protects LAN communications from sniffing, replay, and man-in-the-middle attacks.</p>  |
| <p>P.AUTHORIZATION</p> <p>Users must be authorized before performing Document Processing and administrative functions.</p>   | <p>O.USER_AUTHORIZATION restricts the ability to perform Document Processing and administrative functions to authorized Users.</p> <p>O.USER_I&amp;A provides the basis for authorization.</p> <p>O.ADMIN_ROLES restricts the ability to authorize Users to authorized Administrators.</p> |
| <p>P.AUDIT</p> <p>Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.</p>   | <p>O.AUDIT requires the generation of audit data.</p> <p>O.ACCESS_CONTROL restricts access to audit data in the TOE to authorized Users.</p> <p>O.USER_AUTHORIZATION provides the basis for authorization.</p>   |
| <p>P.COMMS_PROTECTION</p> <p>The TOE must be able to identify itself to other devices on the LAN.</p>  | <p>O.COMMS_PROTECTION protects LAN communications from man-in-the-middle attacks.</p>  |
| <p>P.STORAGE_ENCRYPTION (conditionally mandatory)</p> <p>If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.</p>   | <p>O.STORAGE_ENCRYPTION protects User Document Data and Confidential TSF Data stored in Field-Replaceable Nonvolatile Storage Devices from exposure if a device has been removed from the TOE and its Operational Environment.</p>   |
| <p>P.KEY_MATERIAL (conditionally mandatory)</p> <p>Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.</p> | <p>O.KEY_MATERIAL protects keys and key materials from unauthorized access and ensures that they any key materials are not stored in cleartext on the device that uses those materials for its own encryption.</p>   |
| <p>P.FAX_FLOW (conditionally mandatory)</p> <p>If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.</p>   | <p>O.FAX_NET_SEPARATION requires a separation between the PSTN fax line and the LAN.</p>   |

| Threat/Policy/Assumptions   | Rationale   |
|---|---|
| <p>P.IMAGE_OVERWRITE (optional)</p> <p>Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Device.</p> | <p>O.IMAGE_OVERWRITE overwrites residual image data from Field-Replaceable Nonvolatile Storage Devices after Document Processing jobs are completed or cancelled.</p> |
| <p>A.PHYSICAL</p> <p>Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.</p>                                       | <p>OE.PHYSICAL_PROTECTION establishes a protected physical environment for the TOE.</p>   |
| <p>A.NETWORK</p> <p>The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.</p>  | <p>OE.NETWORK_PROTECTION establishes a protected LAN environment for the TOE.</p>   |
| <p>A.TRUSTED_ADMIN</p> <p>TOE Administrators are trusted to administer the TOE according to site security policies.</p>   | <p>OE.ADMIN_TRUST establishes responsibility of the TOE Owner to have a trusted relationship with Administrators.</p>   |

### 7.3 Security Assurance Requirements rationale

The rationale for choosing these security assurance requirements is that they define a minimum security baseline that is based on the anticipated threat level of the attacker, the security of the Operational Environment in which the TOE is deployed, and the relative value of the TOE itself. The assurance activities throughout the PP are used to provide tailored guidance on the specific expectations for completing the security assurance requirements.