Hewlett-Packard

Security Target

Version 5.6

6/21/2007

Table of Contents

List of Tables

List of Figures

1 Security Target Introduction

This Security Target (ST) describes the Information Technology (IT) security objectives, requirements, and rationale for the identified Target of Evaluation (TOE) and specifies the functional security features and assurance security features of the TOE that meet the stated security requirements. The TOE in this ST is comprised of the device firmware used in a multi-function peripheral (copy and print) with scan to e-mail, scan to folder, scan to analog fax, and analog fax receive capabilities. This device is any of the following:

- HP LaserJet M4345 MFP
- HP LaserJet M3027 MFP
- HP LaserJet M3035 MFP
- HP LaserJet M5025 MFP
- HP LaserJet M5035 MFP
- HP Color LaserJet 4730 MFP

1.1 ST Organization

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and its components.

Chapter 3 provides a security environment description in terms of assumptions, threats, and organizational security policies.

Chapter 4 identifies the security objectives of the TOE and of the IT environment.

Chapter 5 provides functional and assurance security requirements for the TOE, and it lists requirements for the IT environment.

Chapter 6 is the TOE Summary Specification: a description of the functions provided by the TOE to satisfy the security functional and assurance requirements.

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, and TOE summary specification.

1.2 ST and TOE Identification

This section presents the labeling designations that can be used to identify the TOE and this ST.

ST Title:	Hewlett-Packard Security Target for HP LaserJet M4345 MFP System Firmware Version 48.021.7 HP LaserJet M3027 MFP System Firmware Version 48.021.7A HP LaserJet M3035 MFP System Firmware Version 48.021.7A HP LaserJet M5025 MFP System Firmware Version 48.021.7A HP LaserJet M5035 MFP System Firmware Version 48.021.7A HP Color LaserJet 4730 MFP System Firmware Version 46.151.8
ST Version:	5.6
ST Publication Date:	6/21/2007
ST Author:	Hewlett-Packard
TOE Identification:	HP LaserJet M4345 MFP System Firmware Version 48.021.7 HP LaserJet M3027 MFP System Firmware Version 48.021.7A HP LaserJet M3035 MFP System Firmware Version 48.021.7A HP LaserJet M5025 MFP System Firmware Version 48.021.7A HP LaserJet M5035 MFP System Firmware Version 48.021.7A HP Color LaserJet 4730 MFP System Firmware Version 46.151.8
CC Identification:	CC Common Methodology for IT Security Evaluation, Version 2.2, Revision 256, CCIMB-2004-01, ISO/IEC 15408
Assurance Level:	EAL 3
ST Evaluator:	COACT, Inc.
ST Consultant	Criterian Independent Labs
Keywords:	Hewlett-Packard, HP, Color LaserJet 4730, multi-function peripheral, MFP, Secure File Erase, Secure Storage Erase, separation of analog fax from network.

Table: 1.1: ST and TOE identification.

1.3 TOE Overview

The TOE is comprised of the MFP System Firmware. It includes security functionality as it applies to the features listed below:

- **Secure Erase Functionality**. Secure Erase functionality includes Secure File Erase and Secure Storage Erase:
  - Secure File Erase is either of two Secure File Erase modes that cover routine real-time erasing of temporary and permanent files stored on the MFP hard drive and Partition 2 of the MFP Compact Flash card during normal operations such as print, copy, send to email, send to network folder, and fax.
  - Secure Storage Erase is a feature that erases the entire contents of the MFP hard drive or of Partition 2 of the MFP Compact Flash card. Secure Storage Erase deletes files on demand using the Secure File Erase mode that is configured on the MFP.
- **Network and Analog Fax Resource Separation**. The TOE ensures the following regarding network and analog fax resource separation:
  - All data coming in through or going out through the analog fax accessory is only fax data with no network information.
  - All incoming fax data is stored or printed securely.
  - All outgoing fax data is only from the scanner.

- **Identification & Authentication** - Administrators authenticate to the TOE prior to managing security functions.
    - **Management of Security Functions**- The TOE provides for management of security functions. A summary of the TOE security functions appears in Section 2, TOE Description. A detailed description of the security functions appears in Section 6, TOE Summary Specification.

1.4 Conformance to Common Criteria

The TOE conforms to CC Version 2.2, functional requirements (Part 2 extended), and the assurance requirements conform to (Part 3) for EAL 3 level of assurance.

1.5 Protection Profile Conformance

The TOE does not claim conformance to a registered protection profile.

1.6 References

The following documentation was used to prepare this ST:

[CC_PART1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, version 2.2, revision 256, CCIMB-2004-01-001.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security and functional requirements, dated January 2004, version 2.2, CCIMB-2004-01-002.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, version 2.2, revision 256, CCIMB-2004-01-003.

[CEM] Common Methodology for Information Technology Security Evaluation, dated January 2004, version 2.2, revision 256, CCIMB-2004-01-004.

ISO/IEC JTC 1/SC27, Technical Report, ISO/IEC TR 15446, First Edition 2004-07-01, Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets

National Information Assurance Partnership (NIAP) interpretations through January 6, 2006.

1.7 Document Conventions, Glossary, and Acronyms

This section identifies formatting conventions and defines acronyms and terms.

1.7.1 Conventions

The four Common Criteria operations on security functional requirements are documented as follows:

- **Assignments appear in bold**
- Selections appear underlined
- ***Refinements appear in bold with italics***
- Iterations are given unique identifiers by appending (to the component name, short name, and functional element name from the CC) an iteration number inside parenthesis, example: FMT_SMR.1.1 (1) and FMT_SMR.1.1 (2).

1.7.2 Glossary and Acronyms

This ST uses terminology as defined in Section 2.3 of “CC for IT Security Evaluation: Part 1.” The following table defines additional terminology used in this ST:

Term	Definition
Administrator	Someone making configuration changes to the system.
Analog Fax Accessory Package	An add-on analog fax card installed as an upgrade to an HP Color LaserJet 4730 MFP. The package contains a Multi-tech fax modem card and modem firmware that communicates with the analog fax components of the TOE.

Term	Definition
Authorization	Granting administrator access to resource (TOE security management) based on verification of credentials and successful authentication.
CC	Common Criteria for IT security evaluation
CFD	Compact Flash Drive
CM	Configuration Management
EAL	Evaluation Assurance Level
HDD	Hard Disk Drive
HP	Hewlett-Packard
ISO	International Standards Organization
IT	Information Technology
MFP	Multi-Function Peripheral.
NIC	Network Interface Card – The MFP contains an internal Network Interface Card called Jetdirect Inside.
PML	Printer Management Language – an HP proprietary language that operates on HP MFP and printer systems via data objects.
Remanence	The magnetic induction that remains in a material after removal of a magnetizing field.
SNMPv3	An industry-standard security protocol available on the MFP. SNMPv3 is configured according to the Security Checklist.
ST	Security Target
System firmware	HP LaserJet M4345 MFP System Firmware Version 48.021.7 HP LaserJet M3027 MFP System Firmware Version 48.021.7A HP LaserJet M3035 MFP System Firmware Version 48.021.7A HP LaserJet M5025 MFP System Firmware Version 48.021.7A HP LaserJet M5035 MFP System Firmware Version 48.021.7A HP Color LaserJet 4730 MFP System Firmware Version 46.151.8
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
TSC	The set of interactions that can occur with or within a TOE and are subject to the Rules of the TSP are the *TSF Scope of Control (TSC)*. The TSC encompasses a defined set of interactions based on subjects, objects, and operations within the TOE, but it need not encompass all resources of a TOE.
Unauthorized user	Anyone attempting to bypass or violate the TOE Security Policy (TSP).

Table 1.2: Glossary and Acronyms.

2 TOE Description

This section identifies the TOE and the configuration of the TOE that is under evaluation. The TOE resides within the MFP and consists of the MFP System Firmware. The TOE involves firmware features

for erasing files securely on MFP system storage devices. The TOE also includes firmware necessary to ensure that all data coming in through or going out of the analog fax accessory is fax data with no network information, that all fax data coming in is stored or printed securely, and that all fax data going out is from the scanner.

This section defines the physical and logical boundaries of the TOE. It explains authentication requirements necessary to invoke secure erase operations in the TOE. It also discusses the methods by which the TOE protects sensitive data and how the design of the TOE eliminates access to the network from or through the analog fax firmware features or functions. The assumed configuration of the TOE includes implementation of all prescribed settings in the "***HP LaserJet and Color LaserJet MFP Security Checklist,***" which is a guide for configuring MFPs for security in enterprise-level environments. Hereafter, the "***HP LaserJet and Color LaserJet MFP Security Checklist***" is also called the Security Checklist.

2.1 TOE Overview

The TOE is comprised of the MFP System Firmware and includes features that are required to do the following:

- authenticate authorized administrators
- complete secure erase functions
- perform analog fax operations such that all data coming in through or going out of the analog fax accessory is fax data with no network information, that all fax data coming in is stored or printed securely, and that all fax data going out is from the scanner
- management of security functions

2.1.1 Product Type

The TOE consists of the MFP System Firmware, which supports secure erase features, separation of analog fax resources from network resources, authentication, and security management within an MFP. Analog fax accessory packages are accessories to the MFP, but are part of the evaluated configuration.

An MFP is a network peripheral that prints, copies, faxes, and sends scanned documents to email or to network destinations. The TOE is the firmware that enables all properties, features, and components of an MFP.

2.2 Evaluated Configuration

The evaluated configuration is each of the following MFPs configured according to the "***HP LaserJet and Color LaserJet MFP Security Checklist***.:"

- An HP LaserJet M4345 MFP with firmware version 48.021.7 and analog fax accessory package Q3701A
- An HP LaserJet M3027 MFP with firmware version 48.021.7A and analog fax accessory package Q3701A
- An HP LaserJet M3035 MFP with firmware version 48.021.7A and analog fax accessory package Q3701A
- An HP LaserJet M5025 MFP with firmware version 48.021.7A and analog fax accessory package Q3701A
- An HP LaserJet M5035 MFP with firmware version 48.021.7A and analog fax accessory package Q3701A
- An HP Color LaserJet 4730 MFP with firmware version 46.151.8 and analog fax accessory package Q7518A

In each configuration, the Secure File Erase Mode is configured for Secure Fast Erase or for Secure Sanitizing Erase (as prescribed in the Security Checklist).

The fax forwarding option is disabled.

Access to security functions is limited to one authenticated administrator. Users can print, copy, digital send, and fax.

2.3 TOE Physical and Logical Boundaries

This section explains the physical and logical boundaries of the TOE.

2.3.1 Physical Boundary

The physical boundary of the TOE is the MFP System Firmware that resides on Partition 1 of the Compact Flash card, which is mounted on the MFP Formatter Board. Figure 1 illustrates the physical boundaries and its interactions:

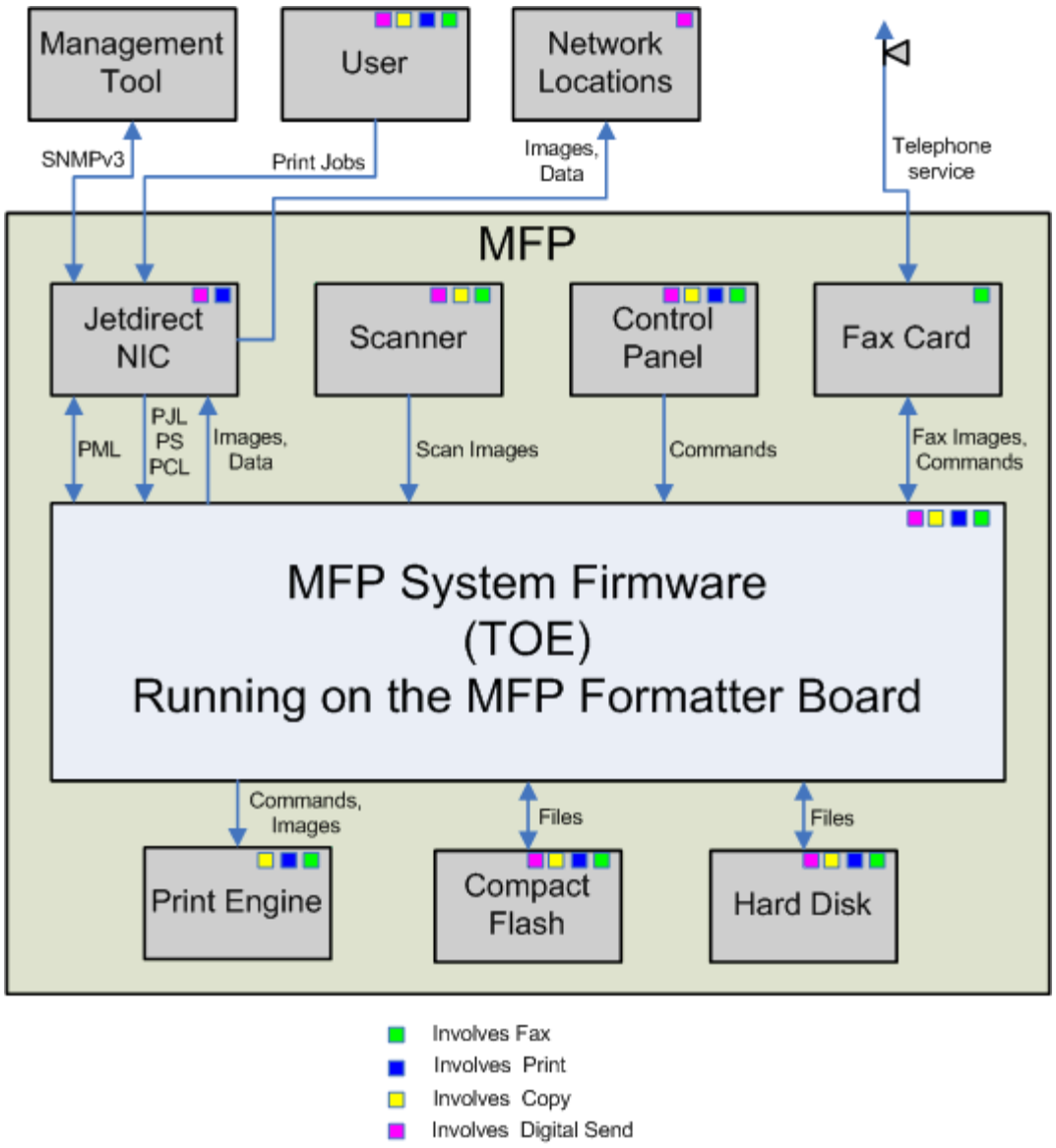

Figure 1: Conceptual system diagram showing the TOE physical boundary, which is labeled MFP System Firmware.

2.3.2 Logical Boundary

The logical boundary of the TOE is the following security features:

- Secure Erase, which provides data protection via Secure File Erase and Secure Storage Erase functionality

- Network and Analog Fax Resource Separation, which ensures that all data coming in through or going out of the analog fax accessory are fax data with no network information, that all fax data coming in through the phone line is stored or printed securely, and that all fax data going out is from the scanner
- Authentication of the administrator
- Management of security features, which includes password configurations, by the administrator

2.4 TOE Components

The MFP System Firmware is the only component of the TOE. The MFP System Firmware consists of all firmware resident on Partition 1 of the Compact Flash Card that is mounted on the formatter printed circuit board inside the MFP. The TOE does not include hardware.

The TOE is any of the following versions of the MFP System Firmware:

- An HP LaserJet M4345 MFP with firmware version 48.021.7
- An HP LaserJet M3027 MFP with firmware version 48.021.7A
- An HP LaserJet M3035 MFP with firmware version 48.021.7A
- An HP LaserJet M5025 MFP with firmware version 48.021.7A
- An HP LaserJet M5035 MFP with firmware version 48.021.7A
- An HP Color LaserJet 4730 MFP with firmware version 46.151.8

The security features in each of these versions of firmware are identical to those in each of the other versions.

NON-TOE Components	Version	Description
Formatter PCB	The released version of the Formatter PCB for each MFP.	The circuit board that controls the main operations of the MFP. The Formatter board includes the Compact Flash card on which the TOE resides.
Fax Card	HP part number Q3943A, HP part number Q7518A, or HP part number Q3701A	A hardware accessory in the form of an add-on I/O card that provides analog fax capability
Compact Flash Drive Partition 2	A virtual partition of the released version of Compact Flash for each MFP	The virtual partition of the MFP Compact Flash drive that contains variables and data that can be deleted using Secure Storage Erase functionality
Compact Flash Drive Partition 1.	A virtual partition of the released version of Compact Flash for each MFP	The virtual partition of the MFP Compact Flash drive that loads firmware and stores variables but is not erased by Secure Storage Erase functionality
Jetdirect Network Interface Card (NIC)	The released version of the MFP embedded Jetdirect NIC	An internal NIC through which all network communication occurs
Print Engine	The released version of the printing mechanism contained in the MFP	The MFP mechanisms that provide functionality for moving media (paper) through the MFP print path and for applying toner onto the media.

NON-TOE Components	Version	Description
Scanner	The released version of the scanning mechanism contained in the MFP	The MFP mechanisms that provide functionality for moving media through the scanner path and for capturing images from media.
Hard Drive	The released version of the Hard Drive that is included with an MFP	A disk drive that stores temporary (user) files, permanent files, and data
Control Panel	The released version of the MFP control panel	The physical interface on the MFP that enables users to interact with the MFP

Table 2.1: Non TOE components.

2.4.1 TOE Logical Components

This section explains the logical components of the MFP:

- Secure Erase
- Network and Analog Fax Resource Separation
- Authentication
- Security Management

These components are explained in the subsections below.

2.4.1.1 **Secure Erase**

The TOE protects residual or remanent information (stored or temporary files used to process print, copy, send to email, send to folder, or fax jobs) by rendering it unavailable to all users by performing Secure Erase operations on the Hard Disk Drive or on Partition 2 of the Compact Flash Drive.

2.4.1.1.1 **Secure File Erase**

Temporary or user files are stored on an MFP hard drive or on Partition 2 of the MFP Compact Flash card during normal operations such as print, copy, scan to email, scan to network folder, and fax. Secure File Erase regulates how the system deletes files. Secure file erase deletes files in real time as jobs of various types (print, copy, send to email, send to folder, or fax) are executed and completed in the system. Secure file erase is called to delete files using one of two optional modes (as configured according to the Security Checklist) for the MFP hard disk drive and one secure mode for Partition 2 of the MFP Compact Flash card:

- Secure Fast Erase – Secure Fast Erase overwrites all addressable locations on the MFP hard disk drive with a single character, providing sufficient security for most network environments.
- Secure Sanitizing Erase – Secure Sanitizing Erase overwrites all addressable locations on the MFP hard disk drive with a character followed by its complement followed by a random character, providing a higher level of security for sensitive environments.
- Secure File Erase for Compact Flash – Secure Erase for Compact Flash overwrites all addressable locations on Partition 2 of the MFP Compact Flash card with a character. Compact flash technology is not magnetic, and it does not exhibit the problem of residual data. When the Secure File Erase setting is configured with either of the secure settings (listed above), the Secure Erase Mode for Compact Flash is used.
  Note that some Compact Flash devices that are supported by the MFPs can accommodate an erase command. In which case, the erase command is used rather than the overwrite function.

2.4.1.1.2 **Secure Storage Erase**

Secure Storage Erase deletes files or data on the entire MFP hard drive or on Partition 2 of the Compact

Flash Drive. It is executed by an administrator on demand. It does not operate continuously. Secure Storage Erase deletes files on the MFP hard drive or in Partition 2 of the MFP Compact Flash card using the mode selected for Secure File Erase, which is either Secure Fast Erase or Secure Sanitizing Erase. The types of files erased include permanent stored jobs, proof and hold jobs, disk-based fonts, and disk-based macro (forms) files.

Note that Secure Storage Erase function for Partition 2 of the MFP Compact Flash card is not the same as that for Secure File Erase. The Secure Storage Erase function treats Partition 2 of the MFP Compact Flash card the same as it treats the MFP hard disk drive. For Secure Fast Erase mode, it overwrites all addressable locations on Partition 2 of the MFP Compact Flash card with one pass. For Secure Sanitize Erase, it overwrites all addressable locations on Partition 2 of the MFP Compact Flash card with three passes.

2.4.1.2 **Network and Analog Fax Resource Separation**

This ST asserts the following properties of MFPs:

- All data coming through or going out through the Analog Fax Accessory is fax data.
- All fax data coming in through the Analog Fax Accessory is stored or printed securely.
- All fax data going out is from the scanner.

These assertions are explained in the subsections below.

2.4.1.2.1 **All data coming in through or going out through the analog fax card is fax data.**

All data that come into or go out of the MFP via the telephone line pass through the fax card. The part of the MFP System Firmware that operates the fax card is a serial modem driver that is exclusive to the fax card. The serial modem driver is also exclusive to fax protocols. No other part of the MFP can open, read, or write to the fax card.

The MFP System Firmware cannot allow generalized communication through the fax card. All requests to send or receive fax data occur only through the fax card and are enabled only when a fax session is active. A fax session is active only when the MFP System Firmware has successfully completed fax negotiation with another fax modem. Fax negotiation occurs when a fax modem calls another fax modem, and the two agree on common capabilities such as resolution, paper size, and format (protocol).

Thus, the MFP is capable of processing fax communication only via the fax card, only in fax protocols, and only with another fax modem to which it is connected and communicating through the telephone service.

2.4.1.2.2 **Ensure that all fax data coming in through the fax accessory is stored or printed securely**

When the MFP System Firmware receives a fax transmission, it cleans up the fax data and writes it to a specific directory that is designated only for incoming fax files. The fax receive, fax print, and the hard disk delete functions of the MFP System Firmware are the only entities permitted to access this designated fax directory. The MFP can store incoming fax transmissions for a limited time to allow for printing at a time that is convenient or secure for users. When the MFP prints the fax, the fax print function can only send the file directly from the designated fax directory to the print engine, which is only capable of printing files. Once printing is complete, the MFP System Firmware erases the file using Secure File Erase. Thus, the MFP can do nothing with an incoming fax transmission other than storing it, printing it, and deleting it.

2.4.1.2.3 **Ensure that all fax data going out is from the scanner**

Data for sending a fax is scanned after command objects are selected in the Control Panel fax UIs. The MFP System Firmware creates a fax job ticket which designates the scan data as a fax job. The MFP System Firmware creates two TIFF versions of the image data each with a different resolution. Then, it writes the two TIFF files to a directory that is designated only for outgoing fax files. There, it stores the files as it opens a fax call and negotiates with a remote fax modem, during which, the resolution is decided. MFP System Firmware sends the TIFF file with the correct resolution to the Fax Card for

sending to the remote fax modem. Once the fax is sent, The MFP System Firmware deletes (securely) both TIFF files.

The fax directories on the MFP Hard Drive are accessible only by the MFP System Firmware functions that process incoming fax transmissions, process outgoing fax transmissions, or delete files. Incoming fax transmissions can only be stored, printed, and deleted. Outgoing fax transmissions can only be stored, sent to the fax card, and deleted. No other entity is permitted access to read or write to the designated fax directories. Thus, all fax data going out of the MFP is from the scanner.

2.4.1.3 Identification & Authentication

This section defines how identification and authentication is handled for secure erase and security management functionality. The MFP (in the evaluation configuration) requires an administrator to authenticate using PML objects (normally invoked from the Jetdirect NIC via SNMPv3 commands) and to provide the File System password before it will allow changes to secure erase options. The TOE compares the user-supplied password to the actual File System password object. If the passwords match, the MFP returns a result of success through PML to the Jetdirect NIC and grants access to the administrator.

The TOE is administered by a single administrative account, which holds an administrative role. Authentication occurs when the administrator provides the File System password.

2.4.1.3.1 PML Interface

The TOE allows the administrator to invoke the Secure File Erase and Secure Storage Erase functions via the PML interface. The administrator does this by sending SNMPv3 commands to the Jetdirect NIC, which converts the SNMPv3 commands to PML objects. The TOE processes the PML objects to activate the functions.

2.4.1.4 Security Management

The TOE allows for security management of Secure Erase functions by requiring restricted access through non-TOE interfaces, which are the only interfaces that can provide these options. This ensures that the secure erase functions are executed as intended by authorized personnel. Only the authenticated and authorized system administrator can enable, disable, or configure the secure file erase or secure storage erase options.

The TOE provides only controlled access to these options. Secure Erase functions cannot be executed without the File System password provided by the authorized system administrator.

2.5 Description of TOE Security Function (TSF) Data and User Data

The following table lists TSF data and user data with their descriptions:

TSF Data	Description
Secure File Erase Mode	A mode set by the administrator to control the type or method of erasure used during routine deleting of files or data. The Evaluation Configuration includes two options for this mode: • Secure Fast Erase • Secure Sanitize Erase
Secure File Erase Blocks to Delete	A quantity of temporary (user) files designated by their locations on the MFP hard drive to delete as ordered by an MFP process (print, copy, fax, send to email, or send to folder). When an MFP process is finished with a block of temporary files, it sends a command to delete that block of data.

TSF Data	Description
Secure Storage Erase Block on which to start delete	The first quantity of data to remove at the time when the entire storage device is erased. The MFP System Firmware stores information on the data block (block/sector 1) on which to begin completely removing all data from an entire device. It removes data blocks sequentially until the device is completely erased.
Fax receive and send directories	Directories on the hard drive where fax image files are stored temporarily until printing or sending. These directories are available only to fax components or to secure erase components.
NVRAM backup information	Information related to system configuration attributes and variables. If the storage device to be erased contains NVRAM backup information, the information is copied to memory (RAM disk file system) on restart.
File System Password	A password associated with authentication for access to Secure Erase configurations. The stored password is compared with the submitted password for access to file system configuration settings in the TOE. This access includes that for secure erase functions. Correct matching of the password is required to make all changes to secure erase functions including changing password, changing the secure erase mode, and executing secure storage erase. Note: The evaluation configuration also requires SNMPv3 credentials which are stored and compared in the Jetdirect NIC.
User Data	Description
Secure File Erase temporary files	Files associated with print, copy, send to email, send to network folder, or fax jobs that are continuously deleted using the Secure File Erase mode after the system is finished processing them.
Secure Storage Erase permanent files	Permanent files stored on either the hard disk or on Partition 2 of the Compact Flash device. Examples: permanent stored jobs proof and hold jobs non-system, non-TSF files such as the following: disk-based fonts disk-based macros (forms)
Fax data received	Data coming in from the analog fax interface. Fax data received is processed only within the analog fax components in fax format. These data are cleaned up or modified slightly before they are written to the hard drive, where they are made available only for printing and erasure.

TSF Data	Description
Fax TIFF image files	TIFF format image files containing sent or received analog fax data. Scanned image files for fax are processed in the form of TIFF format image files. Some received fax files are also TIFF image files. The TIFF files are written to the hard drive, which provides services necessary for transmittal or printing through the fax components.
Fax Job Ticket	A Job ticket specific to a fax formed when a user selects fax menu options from the control panel

Table 2-2: Description of TSF data and user data.

2.6 Rationale for Non-Bypassability and Separation

The TOE is firmware that executes on hardware in the IT Environment. Therefore, responsibility for non-bypassability and separation are split between the TOE and the IT environment.

The TOE provides strictly-controlled functionality to the users within the TSF Scope of Control (TSC). By limiting the functionality, the TSF is protected from corruption or compromise from users within the TSC. The TOE interfaces are separated into two categories: security enforcing and security supporting. Security enforcing interfaces invoke the TSF and ensure that all enforcement functions complete successfully before allowing the user-invoked action to proceed. Security supporting interfaces ensure that the TSF cannot be interfered with via those interfaces (they are isolated from the TSF). Multiple simultaneous users are supported, and the TOE associates distinct attributes and privileges with each process or user to restrict access appropriately.

The TOE and the hardware support non-bypassability by ensuring that access to protected resources passes through the TOE or is limited to access within the TOE scope of control according to the security policies stated for the TOE. The hardware and the TOE provide separate process spaces in which the TOE executes. These process spaces are protected from interference from other processes except through the defined TOE interfaces.

2.7 Restrictions with the Evaluated Configuration

The Evaluated Configuration is achieved by following the HP MFP Security Checklist. The following security-related options are disabled or restricted according to this configuration:

- EWS disabled
- Telnet Config disabled
- SLP Config disabled
- FTP printing disabled
- LPD printing disabled
- IPP printing disabled
- MDNS config disabled
- IPV Multicast disabled
- RCFG access disabled
- IPX/SPX disabled
- AppleTalk disabled
- Printer Firmware Update disabled
- Control panel configuration options disabled
- Access via Digital Send Service disabled
- Direct ports (parallel and USB) disabled

3 TOE Security Environment

This section defines and explains assumptions, threats, and policies applicable to the TOE. Assumptions are conditions that are in place when the TOE is configured and ready for evaluation. Threats are detailed security risks that are due to possible vulnerabilities within the TOE. Security policies are practices, guidelines, and standards applicable to the TOE.

This section identifies assumptions, threats, and policies with the following denotations:

- Assumption: A.[ASSUMPTION]
- Threat: T. [THREAT]
- Policy: P.[POLICY]

3.1 Assumptions

The TOE security environment assumptions are arranged in three areas:

- personnel environment
- physical environment
- IT environment

Personnel environment assumptions describe characteristics of personnel who are relevant to the system.

Physical environment assumptions describe characteristics of the non-IT environment in which the system is deployed.

IT environment assumptions describe the characteristics of the technology environment in which the TOE is operating.

3.1.1 Personnel Environment Assumptions

A.NOEVIL System administrators are competent, non-hostile, not willfully negligent, ongoing, and follow guidance for using the TOE.

3.1.2 Physical Environment Assumptions

A.ENVIRON The MFP is placed in a physical environment where only trusted personnel can access it. The room in which the MFP is operating is a controlled environment where personnel are identified and authorized for access.

3.1.3 IT Environment Assumptions

A.INSTALL The TOE is delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.

A.CHECKLIST The TOE is configured according to the “HP LaserJet and Color LaserJet MFP Security Checklist.”

A.SECURE_COMMUNICATIONS Network communications are protected and authenticated.

A.PROCEDURES Administrators follow established procedures for access, management, administration, and monitoring of the TOE.

3.2 Threats

The threats identified in this section are addressed by the TOE and the Operating IT environment.

3.2.1 TOE Threats

T.RESIDUAL An authorized user may receive residual or remanent information from a previous copy, print, fax, or scan job as the result of a TOE malfunction.

T.TAMPER An unauthorized person tampers with the TOE and accesses sensitive information from a previous copy, print, fax, or scan job.

T.IMPERSONATE An unauthorized person gains access to TOE security management functions by impersonating an administrator.

T.FAXLINE A malicious user attempts to access data or resources via the fax telephone line and modem using publicly available tools and equipment.

3.2.2 Operating IT Environment Threats

TE.RECOVER A malicious user attempts to recover document image data from a print job, a network scan job, or an email job by removing hardware, such as the HDD or the Compact Flash, using readily available tools to read its contents.

TE.TAMPER An unauthorized person attempts to bypass the security mechanism in order to access data or assets on the MFP, to access data or assets on the network, or to disturb or disrupt routine processes on the MFP or on the network.

TE.OPERATION The execution of non-TSF processes such as copying, printing, and digital sending may interfere with TSF processes already running and cause TSF data to be modified, corrupted, or deleted by unauthorized means.

3.3 Policies

No organizational security policies are required for the TOE security environment.

4 Security Objectives

This section identifies the security objectives of the TOE, the IT environment of the TOE, and the non-IT environment of the TOE. The security objectives identify the responsibilities of the TOE. The IT environment of the TOE and the non-IT environment of the TOE identify the ability of the TOE to meet the security needs.

Security Objectives of the TOE are identified as follows:

- Security objectives: O. [OBJECTIVE]
- IT environment objectives: OE. [OBJECTIVE]
- Non-IT environment objectives: ON. [OBJECTIVE]

4.1 TOE Security Objectives

O.RESIDUAL Readable temporary document image data (remanence) from a job does not remain on the hard disk drive once that job is completed.

O.ERASE The TOE completely overwrites image data when files are de-allocated.

O.ADMIN_AUTH The TOE ensures that the administrator is identified or authenticated before it grants the administrator access to the TOE security management functions.

O.SEC_MANAGE The TOE provides all functions necessary to support the authorized administrator in management of TOE security, and the TOE restricts these functions to the administrator.

O.PARTIAL_SELF_PROTECT The TOE is developed to ensure that it enforces policies that protect it against interference, tampering, or bypassing security functions.

O.ON_DEMAND The TOE provides the administrator the ability to invoke the image overwrite function on demand.

O.RESTRICT The TOE restricts access from the telephone line that operates via the TOE's analog fax components to the network and to files within the MFP.

4.2 IT Environment Security Objectives

OE.PHYSICAL The TOE operates in a controlled-access facility. Normal physical access to TOE components is locked. Unauthorized users are not granted access to the facility.

OE.NO_TAMPER The TOE is protected from tampering by non trusted subjects by its lack of access to fax communication resources and to Secure File Erase and Secure Storage Erase configuration settings from the TOE. The only access possible to

fax communication resources is through another fax modem via a phone line. The only access to Secure File Erase and Secure Storage Erase configuration settings is through a secured network connection by an authenticated person.

OE.CORRECT Non-TSF processes operate in cooperation with the TOE. The hardware, the operating system, and other software are dedicated to the TOE and function as documented for the TOE.

OE.MANAGE Documented procedures exist and are followed for securely installing and administering the TOE.

OE.NOEVIL The administrator operates the TOE in the best interest of the environment. The administrator is non-hostile. Users who are granted access to the TOE have low potential for attack.

4.3 Rationale for Security Objectives for the TOE

This section provides the rationale that all security objectives are traced to aspects of the addressed threats.

O.ERASE addresses T.RESIDUAL because overwriting image data destroys all traces of data remaining after removal; thus a user will not have access to residual or remanent data, because it will not exist.

O.ERASE addresses T.TAMPER because overwriting image data when files are deallocated ensures that the data is unavailable; therefore, it cannot be accessed by unauthorized users, it cannot be reused in subsequent jobs, or it cannot be accessed as a result of device malfunction.

O.ADMIN_AUTH addresses T.TAMPER because it ensures that users attempting to access sensitive data or TOE security management functions are authenticated first.

O.SEC_MANAGE addresses T.TAMPER because it ensures that unauthorized users are not permitted access to security management functions.

O.PARTIAL_SELF_PROTECT addresses T.TAMPER because it ensures that unauthorized personnel are denied access to security functions.

O.PARTIAL_SELF_PROTECT addresses T.IMPERSONATE because it ensures that a mechanism for authentication is provided prior to permitting access to TOE security management functions.

O.PARTIAL_SELF_PROTECT addresses T.FAXLINE because it ensures that network policies are in place to keep network traffic separate from fax communications. It also addresses T.FAXLINE because it ensures that they do not communicate with each other or affect each other in any way that can lead to unauthorized access to data or security management functions.

O.ON_DEMAND addresses T.RESIDUAL because it ensures that residual or remanent information is overwritten is such a way to destroy it completely; thus, no one can access it from previous jobs.

O.ON_DEMAND addresses T.TAMPER because it ensures that residual or remanent information is overwritten on demand by the administrator, rendering it unavailable to any subject, object, or operation.

O.RESTRICT addresses T.FAXLINE because it ensures that malicious users cannot access data on the network through the fax telephone line or modem.

O.RESIDUAL addresses T.RESIDUAL because remanent image data from a completed job is destroyed on the hard drive.

	T.RESIDUAL	T.IMPERSONATE	T.TAMPER	T.FAXLINE
O.ERASE	X		X	
O.ADMIN_AUTH			X	
O.SEC_MANAGE			X	
O.PARTIAL_SELF_PROTECT		X	X	X
O.ON_DEMAND	X		X	
O.RESTRICT				X
O.RESIDUAL	X			

Table 4-1: Mappings between Threats and Security Objectives for the TOE.

4.4 Rationale for Security Objectives for the Environment

This section provides the rationale that all security objectives for the environment are traced to aspects of the addressed threats or assumptions.

OE.PHYSICAL addresses TE.RECOVER because it ensures that an attacker does not have access, time, or privacy to access the TOE.

OE.NO_TAMPER addresses TE.TAMPER because it ensures that no method exists to disable or bypass Secure File Erase, Secure Storage Erase, fax, or administrator authorization functions.

OE.NO_TAMPER addresses A.ENVIRON because it ensures that no method exists to access or to disable Secure File Erase configuration settings, Secure Storage Erase configuration settings, or Administrator Authorization functions through the control panel or through external interfaces.

OE.CORRECT addresses A.SECURE_COMMUNICATIONS because the hardware, software, and operating systems are designed and developed properly, they are accurately installed, and they operate properly with protected and authenticated network communications.

OE.CORRECT addresses A.INSTALL because it ensures that the TOE is operates correctly in the expected environment and that it performs correctly according to documentation.

OE.CORRECT addresses TE.OPERATION because the OS and hardware provide a separate execution space for TSF processes. Non-TSF processes cannot execute simultaneously in the same execution space as TSF processes.

OE.CORRECT addresses T.FAXLINE because the OS and hardware do not provide the capability of

communication with the TOE through the fax functionality. Fax functionality is not versatile enough to provide any type of communication other that fax transmissions.

OE.MANAGE addresses A.PROCEDURES because it ensures that documented established procedures are in place for access, management, administration, and monitoring the TOE.

OE.MANAGE addresses A.CHECKLIST because the MFP Security Checklist is required for a configuration that is considered secure.

OE.NOEVIL addresses A.NOEVIL because OE.NOEVIL also provides non-hostile administrators who have low attack potential and operate the TOE in the best interest of the environment.

	A.NOEVIL	A.ENVIRON	A.INSTALL	A.CHECKLIST	A.SECURE COMMUNICATIO	A.PROCEDURES	T.FAXLINE	TE.TAMPER	TE.RECOVER	TE.OPERATION
OE.PHYSICAL									X	
OE.NO_TAMPER		X						X		
OE.CORRECT			X		X		X			X
OE.MANAGE				x		X				
OE.NOEVIL	X									

Table 4-2: Mappings between Threats, Assumptions, and Security Objectives.

5 IT Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

5.1 TOE SFRs

The functional requirements are described in detail in the following subsections. These requirements are also derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.2* with the conventions listed in 1.7.1.

TOE Security Functional Requirements	
FDP_RIP.1	Subset Residual Information Protection
FIA_UID.1	Timing of Identification
FIA_UID.2	User identification before any action
FIA_UAU.1	Timing of Authentication
FIA_UAU.2	User authentication before any action
FMT_SMR.1	Security Roles
FMT_MTD.1	Management of TSF Data
FMT_MOF.1	Management of Security Functions Behavior

TOE Security Functional Requirements	
FMT_SMF.1	Specification of Management Functions

Table 5-1: TOE Security Functional Requirements.

5.1.1 Identification and Authentication (FIA)

This section lists requirements for identification and authentication. Administrators are identified upon authorization in the SNMPv3 tool that is required for access to the TOE (as it is configured correctly for the evaluation configuration), but is not part of the TOE.

The following subsections cover FIAs for this ST:

5.1.1.1 **FIA_UID.1 Timing of Identification**

FIA_UID.1.1 The TSF shall allow [assignment: **none**] on behalf of the ***administrator*** to be performed before the ***administrator*** is identified.

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

Dependencies: No dependencies

5.1.1.2 **FIA_UID.2 User identification before any action**

Hierarchical to: FIA_UID.1

FIA_UID.2.1 The TSF shall require each ***administrator*** to identify itself before allowing any other TSF-mediated actions on behalf of that ***administrator***.

5.1.1.3 **FIA_UAU.1 Timing of Authentication**

Hierarchical to no other components

FIA_UAU.1.1 The TSF shall allow [assignment: **none**] on behalf of the ***administrator*** to be performed before the ***administrator*** is authenticated.

FIA_UAU.1.2 The TSF shall require each ***administrator*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that ***administrator***.

Dependencies: FIA_UID.1

5.1.1.4 **FIA_UAU.2 User authentication before any action**

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 The TSF shall require each ***administrator*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that ***administrator***.

Dependencies: FIA_UID.1

5.1.2 User Data Protection (FDP)

5.1.2.1 **FDP_RIP.1 Subset Residual Information Protection**

Hierarchical to no other components.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects: **hard drive**

Dependencies: No dependencies

5.1.3 Security Management (FMT)

This subsection lists security rules, management of TSF data, management of security functions behavior, and specification of management functions.

5.1.3.1 **FMT_SMR.1 Security Roles**

Hierarchical to no other components.

FMT_SMR.1.1 The TSF shall maintain the role: **administrator**.

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

Dependencies: FIA_UID.1

5.1.3.2 **FMT_MTD.1 Management of TSF Data**

Hierarchical to no other components.

FMT_MTD.1.1 The TSF shall restrict the ability to modify **or set** the **File System password** to the **administrator**.

Dependencies:

FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

Hierarchical to no other components

5.1.3.3 **FMT_MOF.1 Management of Security Functions Behavior**

Hierarchical to: No other components

FMT_MOF.1.1 (1) The TSF shall restrict the ability to disable, enable the functions **Secure File Erase and Secure Storage Erase** to **the administrator**.

FMT_MOF.1.1 (2) The TSF shall restrict the ability to modify the behavior of the functions **Secure Storage Erase** to **the administrator**.

Dependencies:

FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of management functions

5.1.3.4 **FMT_SMF.1 Specification of Management Functions**

Hierarchical to no other components

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

- **Modify the File System password**
- **Enable Secure Fast Erase**
- **Enable Secure Sanitizing Erase**
- **Select the storage drives for Secure Storage Erase**
- **Invoke Secure Storage Erase on demand**

Dependencies: No dependencies

5.2 Security Requirements for the IT Environment

None. This requirement is superseded by explicitly stated SFRs for the environment, Section 5.3.2.

5.3 Explicitly Stated SFRs

5.3.1 Explicitly stated SFRs for the TOE

Explicitly Stated TOE Security Functional Requirements	
EXP_FAX_SEP.1	Network and Analog Fax Resource Separation for TOE
EXP_FDP_DRM.1	Prevention of Data Remanence for TOE
FPT_RVM_SFT.1	Non-Bypassability of the TSP for Software TOEs
FPT_SEP_SFT.1	Domain Separation for Software TOEs

Table 5-2: Explicitly Stated TOE Security Functional Requirements.

5.3.1.1 **EXP_FAX_SEP.1 Network and Analog Fax Resource Separation for TOE**

Hierarchical to no other components

EXP_FAX_SEP.1.1 Access to all network resources or data from the analog fax accessory package through the TSF interface shall be denied.

Rationale for explicitly stated SFR:

This explicitly stated SFR states the portion of network and analog fax resource separation that can be addressed by the TOE and the TOE analog fax components. See EXP_ENV_FAX_SEP (levied on the IT Environment) for the remaining functionality. This SFR addresses the separation of the analog fax components from all other operations of the MFP. The standard SFR that most closely describes this security function is Information Flow control; however, this TOE has no user data to manage, and the Information Flow control SFR does not adequately describe the architecture and stack separation in this case. This explicitly stated requirement addresses the inability of network and analog fax protocols to communicate with each other.

Dependencies: No dependencies+

5.3.1.2 **EXP_FDP_DRM.1 Prevention of Data Remanence for TOE**

Hierarchical to no other components.

EXP_FDP_DRM.1.1 The TSF shall overwrite the entire MFP hard drive or partition 2 of the Compact Flash device as configured by an administrator to ensure that data remanence is destroyed.

EXP_FDP_DRM.1.2 The TSF shall overwrite files or data on demand by an administrator.

Dependencies: No dependencies.

Rationale for Explicitly Stated Requirement:

- The CC does not include an SFR for the removal of data remanence.
- This explicitly stated SFR states the portion of Prevention of Data Remanence that is addressed by TOE. See EXP_ENV_FDP_DRM (levied on the IT Environment) for the remaining functionality.

5.3.1.3 **FPT_ RVM_SFT.1 Non-Bypassability of the TSP for Software TOEs**

Hierarchical to: No other components

FPT_RVM_SFT.1.1 The TSF, when invoked shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

Rationale for explicitly stated SFR:

The TOE is unable to fully satisfy FPT_RVM by itself. This explicitly stated SFR states the portion of FPT_RVM that can be addressed by the TOE. See FPT_RVM_HW (levied on the IT Environment) for the remaining functionality.

5.3.1.4 FPT_SEP_SFT.1 TSF Domain Separation for Software TOE

Hierarchical to no other components.

FPT_SEP_SFT.1.1: The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_SFT.1.2: The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

Rationale for explicitly stated SFR:

This TOE is unable to fully satisfy FPT_SEP by itself. This explicitly stated SFR states the portion of FPT_SEP that can be addressed by the TOE. See FPT_SEP_HW (levied on the IT Environment) for the remaining functionality.

5.3.2 Explicitly stated SFRs for the IT Environment

Explicitly Stated IT Environment SFRs	
EXP_ENV_FDP_DRM.1	Prevention of data remanence for IT Environment
EXP_ENV_FAX_SEP.1	Network and Analog FAX Resource Separation for IT Environment
FPT_RVM_HW.1	Non-Bypassability of the TSP for Hardware
FPT_SEP_HW.1	Domain Separation for Hardware

Table 5-3: Explicitly stated SFRs for the IT environment.

5.3.2.1 EXP_ENV_FDP_DRM.1 Prevention of Data Remanence for IT Environment

Hierarchical to no other components.

EXP_ENV_FDP_DRM.1.1 The IT Environment shall write the buffers specified by the TOE to the MFP hard drive or to Partition 2 of the Compact Flash device at the locations specified by the TOE in support of the function to eliminate data remanence.

Dependencies: No dependencies.

Rationale for Explicitly Stated Requirement:

The CC does not include a Security Functional Requirement for the removal of data remanence.

This explicitly stated SFR states the portion of Prevention of Data Remanence that is addressed by IT Environment. See EXP_FDP_DRM (levied on the IT Environment) for the remaining functionality.

5.3.2.2 EXP_ENV_FAX_SEP.1 Network and Analog FAX Resource Separation for IT Environment

EXP_ENV_FAX_SEP.1.1 Access to any network from the analog fax accessory packages outside the TSF interfaces shall be denied.

Dependencies: No dependencies

Rationale for explicitly stated SFR:

This explicitly stated SFR states the portion of Network and Analog Fax Separation that is addressed by the IT environment and the analog fax accessory package. See EXP_FAX_SEP (levied on the TOE) for

the remaining functionality. This SFR addresses the separation of the analog fax accessory package from the other operations of the MFP. This explicitly stated requirement addresses the inability of network and analog fax protocols to communicate with each other.

5.3.2.3 **FPT_RVM_HW.1 Non-Bypassability of the TSP for Hardware**

Hierarchical to no other components.

FPT_RVM_HW.1.1 The security functions of the hardware shall ensure that the interfaces of the TOE are invoked as stated in this Security Target.

Dependencies: No dependencies

Rationale for explicitly stated SFR:

This TOE is unable to fully satisfy FPT_RVM by itself. This explicitly stated SFR states the portion of FPT_RVM supplied by the hardware in support of the overall FPT_RVM functionality. See FPT_RVM_SFT (levied on the TOE) for the remaining functionality.

5.3.2.4 **FPT_SEP_HW.1 TSF Domain Separation for Hardware**

Hierarchical to no other components.

FPT_SEP_HW.1.1 The security functions of the hardware shall maintain a security domain for TOE execution that protects the TOE from interference and tampering by untrusted subjects in the scope of control of the hardware.

FPT_SEP_HW.1.2 The security functions of the hardware shall enforce separation between the security domains of subjects in the scope of control of the hardware.

Dependencies: No dependencies

Rationale for explicitly stated SFR:

This TOE is unable to fully satisfy FPT_SEP by itself. This explicitly stated SFR states the portion of FPT_SEP supplied by the hardware in support of the overall FPT_SEP functionality. See FPT_SEP_SFT (levied on the TOE) for the remaining functionality.

5.4 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL3 as defined by Part 3 of the CC. These assurance requirements are summarized in the following table:

Security Assurance Requirements		
Assurance Class	**Component ID**	**Component Title**
Configuration Management	ACM_CAP.3	Authorization Controls
Configuration Management	ACM_SCP.1	TOE CM Coverage
Delivery and Operation	ADO_DEL.1	Delivery Procedures
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures
Development	ADV_FSP.1	Informal Functional Specification
Development	ADV_HLD.2	Security Enforcing High-Level Design
Development	ADV_RCR.1	Informal Correspondence Demonstration
Guidance Documents	AGD_ADM.1	Administrator Guidance
Guidance Documents	AGD_USR.1	User Guidance

Security Assurance Requirements		
Life Cycle Support	ALC_DVS.1	Identification of Security Measures
Tests	ATE_COV.2	Analysis of Coverage
Tests	ATE_DPT.1	Testing: High-Level Design
Tests	ATE_FUN.1	Functional Testing
Tests	ATE_IND.2	Independent Testing – Sample
Vulnerability Assessment	AVA_MSU.1	Examination of Guidance
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis

Table 5-4: Security Assurance Requirements.

5.5 TOE SOF Declarations

The only probabilistic or permutational mechanism in the MFP is the password mechanism used to authenticate the administrator. The claimed minimum strength of function is SOF-basic. FIA_UAU.1 is the only TOE security functional requirement that depends on this permutational function.

5.6 Rationale for TOE Security Functional Requirements

This section provides rationale for the chosen SFRs, and it demonstrates how each security objective is enforced by the SFRs.

FDP_RIP.1 supports O.RESIDUAL because data remaining on the hard drive from temporary job files are completely overwritten once each job is completed.

FDP_RIP.1 supports O.ERASE because temporary and permanent files on the hard drive are completely overwritten continuously upon completion of each job that creates the files.

FIA_UID.1 supports O.ADMIN_AUTH because it ensures that each user is identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2 supports O.ADMIN_AUTH because it ensures that each user is identified before allowing any actions on behalf of that user.

FIA_UAU.1 supports O.ADMIN_AUTH because it ensures that each user is authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 supports O.ADMIN_AUTH because it ensures that each user is authenticated before allowing any actions on behalf of that user.

FMT_MOF.1 supports O.SEC_MANAGE because it prevents unauthorized users from accessing options for enabling, disabling, or modifying the behavior of Secure Erase functions.

FMT_MTD.1 supports O.SEC_MANAGE because it prevents unauthorized users from accessing options for changing the Files System password. Only the administrator can set or modify the password, which is TSF data.

FMT_SMF.1 supports O.SEC_MANAGE because it defines the TOE Security Management functions for which to restrict access. TSF manages access to the Secure Erase and Password Management functions of the TOE, which implements the authentication mechanism.

FMT_SMR.1 supports O.SEC_MANAGE because the TOE maintains the ability to recognize the administrative role and allow only administrator access to functions and facilities that manage TOE security.

EXP_FAX_SEP.1 supports O.RESTRICT as it restricts the internal network from the analog fax

component interfaces. Access to the internal network and user data in the MFP is not possible due to the architecture of the analog fax components and the inability of fax protocols to communicate with network protocols.

EXP_FDP_DRM.1 supports O.ERASE because it ensures that sensitive data is erased by overwriting the storage drives with characters.

EXP_FDP_DRM.1 supports O.ON_DEMAND because it ensures that sensitive data is made unavailable when the administrator performs an overwrite operation with Secure Storage Erase.

EXP_FDP_DRM.1 supports O.RESIDUAL by ensuring that image data (remanence) from completed jobs is destroyed on the hard drive.

FPT_RVM_SFT.1 supports O.PARTIAL_SELF_PROTECT as the TOE enforces non-bypassability of the TSP by ensuring that all authorized security functions are invoked and succeed, which provides that untrusted subjects are prevented from performing any other function within the TSC.

FPT_SEP_SFT.1 supports O.PARTIAL_SELF_PROTECT because the TOE security functions are not accessible through the phone line. Thus it is protected from interference with fax communication through the network, and it is protected against interference with network communication through the phone line.

FPT_SEP_SFT.1 supports O.RESTRICT because the TOE maintains a security domain that is not accessible through the phone line. Thus, it is protected from interference and tampering by unauthorized users of the TOE through telephone interfaces.

The following table contains a mapping of the functional requirements and the security objectives each requirement enforces.

	O.RESIDUAL	O.ERASE	O.PARTIAL_SELF_PROTECT	O.ADMIN_AUTH	O.SEC_MANAGE	O.ON_DEMAND	O.RESTRICT
FDP_RIP.1	X	X					
FIA_UID.1				X			
FIA_UID.2				X			
FIA_UAU.1				X			
FIA_UAU.2				X			
FMT_MOF.1					X		
FMT_MTD.1					X		
FMT_SMF.1					X		
FMT_SMR.1					X		
EXP_FAX_SEP.1							X
EXP_FDP_DRM.1	X	X				X	
FPT_RVM_SFT.1			X				
FPT_SEP_SFT.1			X				X

Table 5-5: Mapping of TOE Functional Requirements to Objectives.

5.7 Rationale for TOE Security Requirements

EAL3 was chosen to provide a basic level of independently assured security. The chosen assurance level is consistent with the postulated threat environment, specifically, that the threat of malicious attacks is low and that the product will have undergone a search for obvious flaws.

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is as follows:

- is consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market
- meets current constraints on widespread acceptance by expressing its claims against EAL3 from part 3 of the Common Criteria

5.8 Rationale for IT Environment Security Requirements

This section lists the functional requirements levied on the environment and the security objectives satisfied by the environment that each requirement enforces.

EXP_ENV_FAX_SEP.1 supports OE.NOTAMPER because the only way to access fax communication is by sending a fax from another fax modem. The TOE fax functionality is capable of reading only fax packets that come from another fax modem. There is no way to tamper with fax communication functions by anyone. Thus integrity of the fax TSF functions is protected by the lack of access.

FPT_RVM_HW.1 supports OE.NO_TAMPER because the hardware is designed to exclude unauthorized access to the security domain. No access exists to interfere with fax communication, and only the authorized administrator can access configuration options for Secure File Erase or Secure Storage Erase.

EXP_ENV_FDP_DRM.1 supports OE.CORRECT because the correct functioning of the firmware (hardware and software) of the MFP ensures that the firmware includes code that requires data to be written to specific directories on the hard drive. The Secure File Erase and Secure Storage Erase code is designed to look for data in those specific locations.

FPT_RVM_HW.1 supports OE.CORRECT because the security functions of the hardware shall operate correctly to ensure that hardware security policy enforcement functions are invoked and succeed before each function within the scope of control of the hardware is allowed to proceed.

FPT_SEP_HW.1 supports OE.NO_TAMPER because it prevents everyone from accessing fax capabilities for anything other than sending or receiving fax transmissions.

The following table maps the functional requirements and the security objectives each requirement enforces:

	OE.NO_TAMPER	OE.CORRECT
EXP_ENV_FAX_SEP.1	X	
FPT_RVM_HW.1	X	X
FPT_SEP_HW.1	X	
FPT_ENV_FDP_DRM.1		X

Table 5-6: Mappings between Functional Requirements and Objectives.

5.9 Rationale CC Component Hierarchies and Dependencies

This section demonstrates that the identified SFRs include the appropriate hierarchy and dependencies.

5.9.1 TOE Security Functional Component Hierarchies and Dependencies

The following table lists the TOE SFRs, the SFRs to which they are hierarchical, the SFRs on which they are dependent, and the rationale:

SFR	Hierarchical To	Dependency	Rationale
FDP_RIP.1	No other components.	None	Yes
FIA_UID.1	No other components	None	Yes
FIA_UID.2	FIA_UID.1	None	Yes

SFR	Hierarchical To	Dependency	Rationale
FIA_UAU.1	None	FIA_UID.1	Yes
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Yes
FMT_MOF.1	No other components	FMT_SMF.1, FMT_SMR.1	Yes Yes
FMT_MTD.1	No other components	FMT_SMF.1, FMT_SMR.1	Yes Yes
FMT_SMF.1	No other components	None	N/A
FMT_SMR.1	No other components	FIA_UID.1	Yes
EXP_FAX_SEP.1	No other components	None	n/a
EXP_FDP_DRM.1	No other components	None	n/a
FPT_RVM_SFT.1	No other components	None	n/a
FPT_SEP_SFT.1	No other components	None	n/a

Table 5-7: TOE Security Functional Component Hierarchies and Dependencies.

5.9.2 IT Environment Security Functional Component Hierarchies and Dependencies

This section demonstrates that the identified IT SFRs include the appropriate hierarchy and dependencies.

The following table lists the IT SFRs and the SFRs to which each is hierarchical, dependent on necessary rationale:

SFR	Hierarchical To	Dependency	Rationale
EXP_ENV_FAX_SEP.1	No other components	None	n/a
EXP_ENV_FDP_DRM.1	No other components	None	n/a
FPT_RVM_HW.1	No other components	None	n/a
FPT_SEP_HW.1	No other components	None	n/a

Table 5-8: IT Security Functional Component Hierarchies and Dependencies.

5.10 Rationale for Strength of Function Claim

The claimed minimum strength of function is SOF-basic. The authorization requirements in FIA_UAU.1 contain a permutational function requiring SOF analysis. SOF-basic is defined in CC Part 1 section 2.3 as follows: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential."

The rationale for the chosen level is based on the low attack potential of the threat agents identified in this ST.

6 TOE Summary Specification

This section presents an overview of the security functions implemented by the TOE and the Assurance Measures applied to ensure the correct implementation of the security functions.

6.1 TOE Security Functions

This section describes the security functions performed by the TOE in order to satisfy the SFRs identified in section 5.1.1. Each description traces the TSF to one or more SFRs that are satisfied by the TSF.

6.1.1 Secure File Erase

With the secure file erase mode set to a secure mode, files that have been written to the hard drive during print, copy, send to email, send to network folder, or fax operations are overwritten in real time when the MFP is finished processing the files.

6.1.1.1 **Secure File Erase Modes**

The Evaluation Configuration requires the administrator to change the factory default Secure File erase mode to either of the following options (according to "***HP LaserJet and Color LaserJet MFP Security Checklist***"):

- Secure Fast Erase
- Secure Sanitizing Erase

6.1.1.1.1 **Secure Fast Erase**

Secure Fast Erase is the Secure File Erase mode by which all addressable file locations are overwritten once with a character. This mode provides sufficient security for most network environments.

6.1.1.1.2 **Secure Sanitizing Erase**

Secure Sanitizing Erase is the Secure File Erase mode by which file locations are overwritten with three passes using a secure, repetitive method to remove all residual or remanent data as a file is deleted. The first pass is a character written to each byte of each deleted sector. The second pass is the complement of the first character written to each byte of each deleted sector. The third pass is a random character written to each byte of each deleted sector. This mode provides a higher level of security for sensitive network environments that require it.

Note that this method is not used for deleting files on Partition 2 of the MFP Compact Flash device since Compact Flash technology is not magnetic and does not exhibit the problem of data remanence. When the Secure File Erase mode is set to either Secure Fast Erase or to Secure Sanitizing Erase, files deleted on the MFP Compact Flash device are overwritten one time with a character.

SFRs Satisfied: FDP_RIP.1, EXP_FSP_DRM.1

6.1.2 Secure Storage Erase

With the MFP in the Evaluation Configuration (Secure File Erase mode set to Secure Fast Erase or to Secure Sanitize Erase), the Secure Storage Erase feature enables administrators to delete (overwrite) all permanent, user job-related data, and non-system data files from the Hard Disk Drive or from Partition 2 on the Compact Flash Drive on demand. The Secure Storage Erase feature synchronizes to the Secure File Erase mode (see description above) that is configured for the MFP.

The MFP stores various types of files on its hard drive and on Partition 2 of its Compact Flash drive for various reasons. These files include permanent files, user job-related data files, and all other non-system data files. The files that are called permanent files include stored jobs, proof and hold jobs, disk-based fonts, and disk-based macros (forms). User job-related files include temporary image files that are required to complete print jobs, copy jobs, send-to-email jobs, send-to-network folder jobs, or fax jobs. The MFP may also store other non-system data files on the storage drives. Secure Storage Erase destroys all of these files and all other data, except for critical system variables, from the hard disk drive or from Partition 2 of the Compact Flash drive on demand by the administrator. During this process for the MFP hard disk drive, Secure Storage Erase uses the Secure File Erase mode (method) that is configured for the MFP to delete (destroy) the information.

Note that Secure Storage Erase uses the same method for deleting the data on Partition 2 of the MFP Compact Flash drive that is used for deleting the data on the MFP hard disk drive. If Secure Fast Erase is configured for the Secure File Erase setting, Secure Storage Erase will overwrite the data on Partition 2 of the MFP Compact Flash device with one pass. If Secure Sanitizing Erase is configured for Secure File Erase, Secure Storage Erase will overwrite the data on Partition 2 of the MFP Compact Flash device with 3 passes.

Secure Storage Erase reboots the MFP. During this reboot, the MFP System Firmware skips mounting the storage device that is scheduled for the overwrite operation. This allows the Secure Storage Erase feature to have full access to the storage device. This also causes other MFP services to become unavailable during the operation. As the process continues, all sectors of the storage device that contain permanent, non-system, or user job-related data are overwritten. When overwriting is finished, the MFP reboots again to remount the storage device normally and to enable regular MFP operations.

If the MFP is turned off after beginning a scheduled Secure Storage Erase operation, the MFP will continue to attempt the operation until it is successful. If power to the MFP is lost during a Secure Storage Erase operation, the MFP will restart the Secure Storage Erase operation on reboot starting at the first block and continuing sequentially until completed.

SFRs Satisfied: EXP_FDP_DRM.1

6.1.3 Identification & Authentication

Identification and Authentication is required for management of the security functions, including the Secure File Erase and Secure Storage Erase configuration options. To make changes to these configuration options, an administrator provides the correct File System Password through an SNMPv3 tool. The SNMPv3 commands are received by the Jetdirect NIC, where they are translated to PML objects. The TOE process the PML objects and performs a comparison between the PML File System password object received from the Jetdirect NIC and the File System password object stored on the MFP. The comparison must return a match before the MFP will allow the command to change the configuration options.

The TOE relies on operational controls to authorize users to the administrative role (A.PROCEDURES). The TOE is administered by a single administrative account, which holds the administrative role; therefore, authentication occurs when the administrator provides the File System Password (as described above).

SFRs Satisfied: FIA_UAU.1, FIA_UAU.2, FIA_UID.1, FIA_UID.2

6.1.4 Security Management

The administrator manages security features remotely using an SNMPv3 tool outside the TOE. The only method to provide security management UIs for the TOE is via an SNMPv3 tool.

Only the authenticated administrator (who has the file system password) can remotely manage security features such as the secure erase functions. This is because the TOE allows no changes to secure erase functions unless the correct File System Password is set. The TOE requires that a request to change a secure storage erase option is preceded by a validation that the user has the correct original File System password. If the administrator provides an incorrect File System Password, the TOE responds with an error. If the password is incorrect again, the TOE responds with the same error.

Once the File System Password is set (by an authorized administrator), the MFP requires it before it grants access to modify the password or to modify File System options. The TOE requires that a request to change the password is preceded by a validation that the user has the correct original File System password. If the correct original password is not provided, the TOE responds with an error. When the correct File System Password is provided, the TOE allows one configuration change. The TOE requires authentication again to make a second change.

The following table lists many of the manageable security features with their possible variables:

Feature	Options	Parameters	Purposes
File System Access Control	File system password	One or more characters up to 8, after which, all characters are truncated	Requires the password before granting access to make changes to the file system features.
Secure File Erase	Secure File Erase Mode setting	Secure fast erase Secure sanitize erase	Configures the continuous mode by which files are deleted from storage devices
Secure Storage Erase	The storage device to erase	Hard disk Other media (apply button executes)	Executes Secure Storage Erase feature on selected storage devices on demand.

Table 6-1: Security features with options, parameters, and purposes.

SFRs Satisfied: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

6.1.5 Network and Analog Fax Resource Separation

Network and Analog Fax Resource Separation is a function of the TOE. It includes analog fax features and properties that are necessary to prove that altering or accessing network resources through fax access points are not possible.

6.1.5.1 **Ensure That All Data Coming in through or going out of the Analog Fax Accessory is Fax Data with No Network Information**

Data does not come into or go out of the analog fax accessory except through the serial fax modem. The only components in the MFP that can open, read, or write to the serial fax modem are inside the TOE, are specific to that purpose, and are the only components that can open the modem device or operate it in any way.

The functions of the TOE that read or write bytes to the modem are strictly specific to fax functionality. They cannot allow generalized communication through the modem. The TOE requires that all requests to send or receive data through the fax accessory occur only during an active fax session. A fax session becomes active when the TOE successfully completes fax negotiation with another fax modem (When fax modems call one another, they negotiate for agreement on common capabilities such as fax resolution, paper size, and format. Both modems must agree on format, and no format other than analog fax is available). Fax negotiation and communication occur only using T.30 protocol, which is specific to fax communication. Therefore, if an attacker attempts to make a call to or from an MFP fax modem to try to access the network, no part of the call can be negotiated since it cannot apply to a fax session. A fax session cannot be activated for anything other than a fax transfer, and there is no way for any other existing component in or out of the system to use the modem for transferring data other than fax data.

6.1.5.2 **Ensure that all fax data coming in is stored or printed securely**

The TOE writes received fax data files to only one directory on the hard drive where they are stored until printed and then deleted. At the time of printing, the MFP System Firmware sends the fax file from the fax directory directly to the print spooler.

The design of the MFP System Firmware prohibits all other paths for received fax data. The only way the path for received fax data could be altered is by altering the firmware code, which requires intricate knowledge of the MFP – something an attacker would not likely have.

An attacker on the network could potentially access the hard drive directory and delete, modify, or copy

files that will could picked up by the Fax functionality and printed. This would require specific knowledge with access to the hard drive and understanding of the timing required to access temporary fax files and to know the directory where incoming fax files are stored. An attacker with average skills will be denied access to the hard drive when attempting to use the Evaluated Configuration.

6.1.5.3 **Ensure that all fax data going out is from the scanner**

All data for sending a fax is scanned on the MFP scanner from command objects selected in the Control Panel fax UIs. The TOE creates a fax job ticket, translates the data, and creates two versions of a TIFF image file each with a different resolution. Then, the TOE writes the two TIFF image files to a directory on the hard drive specifically designated only for fax files. There, the files are stored during fax negotiation with the remote fax modem. During negotiation, the resolution is decided. The TOE picks up the TIFF file that has the agreed resolution converts it to fax protocol packets, and sends it out through the fax modem. Once the fax is sent, both TIFF files are securely deleted from the hard drive.

The firmware design prohibits having any other path for sent fax data. The only way the data path for sent fax data could be altered is by altering the firmware code, which requires intricate knowledge of the MFP – something an attacker likely would not have.

An attacker on the network could potentially access the directory on the hard drive and delete, modify, or copy files that could be picked up and sent out through the fax card; however, this would require specific knowledge of the MFP because the attacker must have access to the hard drive and know the exact directory where the outgoing fax files are stored. An average attacker using the Evaluated Configuration is denied access to the hard drive.

The Analog Fax functions of the TOE are designed only to send and receive analog fax data for the MFP. In order to send and receive faxes, the Analog Fax Accessory package employs a standard fax/data modem card that interfaces using fax protocols through an internal serial port. The closed nature of analog fax firmware with its limited functionality does not provide a pathway or support for commands necessary to achieve network access.

The third-party Multi-tech analog fax card can plug into only one designated serial port on the MFP formatter board and to an external phone line. The Analog Fax Accessory package converts an incoming fax to a digital image and transfers the image data to the MFP via the designated serial connection. The modem control functions of the TOE use a parallel GPIO driver to control the analog fax card and to synchronize the two devices.

The fax modem, contained in the analog fax accessory package, is installed on a serial port, and, thus, is managed as a serial device. The only components in the MFP that can open, read, or write to a serial modem are specific to fax functionality. Thus, no other process or functions can operate the modem in any way.

The MFP System Firmware requires that all requests to send or receive fax data occur only when a fax session is active. A fax session must successfully complete negotiation to become active. When a fax modem calls another fax modem, the two negotiate to identify their common capabilities such as fax resolution and paper sizes. Therefore, if an attacker attempted to make a call to or from an MFP fax modem to try to access the network, no part of the call could be negotiated since it cannot apply to a fax data session. A fax session cannot be activated for anything but a fax transfer. There is no way for any other existing component in or out of the system to use the modem for transferring data other than fax data.

The TOE's architecture and design provide separation between the analog fax processing board and the network controller. Faxes from a phone line cannot be sent into the network, and they cannot influence other resources on the network.

This feature is articulated by the explicitly stated SFR, EXP_FAX_SEP.1 - Network and Analog Fax Resource separation.

SFRs Satisfied: EXP_FAX_SEP.1, FPT_SEP_SFT.1, FPT_RVM_SFT.1

6.2 TOE Security Assurance Measures

The assurance level selected for the TOE is EAL3 because EAL3 is applicable in circumstances where users require a moderate level of independently-assured security and where the evaluation requires a thorough investigation of the TOE and its development without substantial re-engineering. EAL3 provides assurance by analysis of the security functions using a functional and interface specification, guidance documentation, and the high-level design of the TOE to explain the security behavior.

EAL3 analysis is supported by the following:

- independent testing of the TOE security functions
- evidence of developer testing based on the functional specification and high-level design
- selective independent confirmation of the developer test results
- strength of function analysis
- evidence of a developer search for obvious vulnerabilities

Appropriate assurance measures are employed to satisfy the security assurance requirements. The TOE evaluation confirms that the assurance measures are sufficient to satisfy the assurance requirements.

The assurance measures are described in the set of evaluation evidence listed in Table 6-1, below. The documents listed in the table were used to satisfy assurance evaluation requirements.

Assurance Component/Name	**Evaluation Evidence (*note; names may change as these docs are developed)***	**Rationale**
ACM_CAP.3 Configuration Management	TOE CM Coverage	The following Configuration Management procedures are described in this documentation: Use of the CVS tool for revision control Use of documented procedures for product builds Use of documented procedures for product test Use of documented procedures for release to manufacturing Use of documented procedures for distribution to customers List of configuration items and evidence that they are maintained by the CVS tool.
ACM_SCP.1 Configuration Management	TOE CM Coverage	This document contains lists of the items tracked by the CVS revision control tool. These items include the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.
ADO_DEL.1 Delivery and Operation	Delivery Procedures	This document includes descriptions of the process used to create distribution copies of the TOE and the procedures used to ensure consistent delivery of the TOE.

Assurance Component/Name	**Evaluation Evidence (*note; names may change as these docs are developed)***	**Rationale**
ADO_IGS.1 Installation	Installation Guide (HP LaserJet and Color LaserJet MFP Security Checklist)	This document describes the procedures necessary for secure installation, generation, and start-up of the TOE.
ADV_FSP.1 Functional Specification	Informal Functional Specification	This document provides the purpose and method of use of each external TSF interface and completely represents the TSF.
ADV_HLD.2 High Level Design	Security Enforcing High Level Design	This document describes the high level design. It contains a representation of the TSF in terms of subsystems, identifying the TSP-enforcing subsystems and the security functions. All subsystem interfaces are identified, and the externally visible interfaces are noted. The purpose and method of use of each interface to the TSF subsystems is described.
ADV_RCR.1 Development	Informal Correspondence Demonstration	This document describes the correspondence between the TOE security functions and the functional specification and the correspondence between the functional specification and the high-level design subsystems.
AGD_ADM.1 Administrative Guidance	Administrative Guidance	Guidance to administrators is effectively supported by the listed documentation for this requirement.
AGD_USR.1 User Guidance	User Guidance	Guidance to non-administrative users is effectively supported by the listed documentation for this requirement.
ALC_DVS.1 Development	Life Cycle Support	This document describes the security measures employed to protect the confidentiality and integrity of the TOE design and implementation and to provide evidence that the measures are used.
ATE_COV.2 Tests	Analysis of Coverage	This document describes the functional and penetration tests performed and the security functions they cover.
ATE_DPT.1 Tests	Analysis of Depth Coverage	This document describes the functional and penetration tests performed and the subsystems they cover.
ATE_FUN.1 Tests	Functional Testing	This document describes the developer's functional and penetration tests performed and their results.

Assurance Component/Name	Evaluation Evidence (*note; names may change as these docs are developed)*	Rationale
ATE_IND.2 Tests	Independent Testing	This document describes the functional and penetration tests performed and their results.
AVA_MSU.1 Strength of Function Analysis and Vulnerability Assessment	Examination of Guidance	This document describes whether an administrator or user with an understanding of the guidance documentation is able to determine if the TOE is configured and operating in a manner that is secure.
AVA_SOF.1 Strength of Function Analysis	Strength of TOE Security Function Evaluation	This document includes a-strength of-function analysis to support the SOF basic claim. The analysis includes identifying the TOE password space and the probability of a password being compromised.
AVA_VLA.1 Vulnerability Assessment	Developer Vulnerability Analysis	This document describes the vulnerability analysis performed and the results of the analysis.

Table 6-1 Evaluation Evidence for Assurance Requirements

6.3 Rationale for TOE Security Functions

The following section provides a rationale supporting the way in which each security function ensures the satisfaction of each implementation-independent Security Functional Requirement.

FDP_RIP.1	Subset Residual Information Protection. The Secure File Erase feature ensures that, when the Secure Sanitizing Erase mode of the Secure Erase function is chosen, all residual information is deallocated upon release.
FIA_UID.1	Dependency of FIA_UAU.1 and FIA_UAU.2
FIA_UID.2	Hierarchical to FIA_UID.1
FIA_UAU.1	Timing of user authentication. The authentication feature involved in the TOE checks for a match between the File System Password PML object supplied by the MFP and the File System Password supplied by the administrator via the SNMPv3 tool.
FIA_UAU.2	User authentication before any action. The authentication feature involved in the TOE checks for a match between the File System Password PML object supplied by the MFP and the File System Password supplied by the administrator via the SNMPv3 tool.
FMT_MOF.1	Management of Security Functions Behavior. The Security Management feature supports FMT_MOF.1 by ensuring that only administrators can enable, modify, or determine the behavior of Secure File Erase and Secure Storage Erase and by describing the administrator's ability to configure the Secure Erase features.
FMT_MTD.1	Management of TSF Data. The Security Management feature supports FMT_MTD.1 by allowing only administrators access to management of the File System Password and to the Secure Erase features.
FMT_SMF.1	Specification of Management Functions. The Security Management feature supports FMT_SMF.1 by describing the administrator's ability of the TSF to set or

	modify the File System Password, to set the Secure File Erase mode to Secure Fast Erase or Secure Sanitizing Erase, to specify a storage device to erase, and to erase the specified storage device on demand.
FMT_SMR.1	Security Roles. The Security Management feature supports FMT_SMR.1 by ensuring that the administrator is the only security role.
EXP_FAX_SEP.1	Network and Analog Fax Resource Separation supports the explicitly-stated SFR, EXP_FAX_SEP, because it denies access to the internal network from the TOE analog fax component interfaces.
EXP_FDP_DRM.1	Secure File Erase supports the explicitly-stated EXP_FDP_DRM.1 because each of the two Secure File Erase Modes, Secure Fast Erase and Secure Sanitizing Erase, perform an overwrite process for removing data remanence.
EXP_FDP_DRM.1	Secure Storage Erase supports the explicitly-stated EXP_FDP_DRM.1 because it removes all non-system data from the storage devices by performing an overwrite process of the data. It performs the overwrite process according to the selected Secure File Erase mode (Secure Fast Erase or Secure Sanitizing Erase).
FPT_RVM_SFT.1	Non-Bypassability of the TSP for Software TOEs. The network and analog fax resource separation supports FPT_RVM_SFT.1 because it provides no interfaces between fax components and network components. The TOE provides no access to network components via fax interfaces, and it provides no access to fax components via network interfaces. Fax protocols and fax processes enforce that only fax transactions occur on fax interfaces. These interfaces are not capable of handling network traffic because they require all transactions through them to be done via telephone and only via fax modem to fax modem. Network protocols and processes do not match fax protocols and processes, and, therefore, are not permitted in fax transactions.
FPT_SEP_SFT.1	Network and Analog Fax Resource Separation supports the explicitly-stated SFR, FPT_SEP_SFT.1, by maintaining a security domain protected from interference and tampering by non-trusted subjects in the TSC by providing no method of access to fax interfaces via network interfaces and no method of access from network interfaces to fax interfaces. The design if the TOE allows no such access. No subjects, untrusted or trusted, can obtain access.

The following table shows the mapping between the Security Functional Requirements and the security functions provided by the TOE, which are listed above.

	Secure File Erase	Secure Storage Erase	Identification and Authentication	Security Management	Network/Analog Fax Resource Separation
FDP_RIP.1	X				
FIA_UID.1			X		
FIA_UID.2			X		

	Secure File Erase	Secure Storage Erase	Identification and Authentication	Security Management	Network/Analog Fax Resource Separation
FIA_UAU.1			X		
FIA_UAU.2			X		
FMT_MOF.1				X	
FMT_MTD.1				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
EXP_FAX_SEP.1					X
EXP_FDP_DRM.1	X	X			
FPT_RVM_SFT.1					X
FPT_SEP_SFT.1					X

Table 6-2 Mapping of Security Functional Requirements to Security Functions

7 PP Claims

The TOE claims no PP conformance.

8 Rationale

This chapter provides rationale for the selection of the IT security requirements, objectives, assumptions, and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional requirements.

8.1 Rationale for IT Security Objectives

Section 4.3 and 4.4 of the ST demonstrate that the identified security objectives cover all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

8.1.1 Rationale Showing Threats to Security Objectives

Section 4.3 describes the rationale for the threat-to-security objectives mapping.

8.1.2 Rationale Showing Assumptions to Environment Security Objectives

Section 4.4 describes the rationale for the assumption-to-security objectives mapping.

8.2 Security Requirements Rationale

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

Section 5.6 provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

8.2.2 Rationale for Security Functional Requirements of the IT Environment Objectives

Section 5.8 provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the IT security objectives.

8.2.3 SOF Rationale

See Section 5.10 for SOF Rationale.

8.2.4 Security Assurance Requirements Rationale

8.2.4.1 **TOE Security Assurance Requirements Rationale**

The TOE meets the assurance requirements for EAL3. The following table provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Component ID	Rationale
ACM_CAP.3	This document describes the following Configuration Management procedures: • Use of the CVS tool for revision control • Use of documented procedures for product builds • Use of documented procedures for product test • Use of documented procedures for release to manufacturing • Use of documented procedures for distribution to customers • List of configuration items and evidence that they are maintained by the CVS tool.
ADO_DEL.1	This document includes descriptions of the process used to create distribution copies of the TOE and the procedures used to ensure consistent delivery of the TOE.
ADO_IGS.1	This document describes the procedures necessary for secure installation, generation, and start-up of the TOE.
ADV_FSP.1	This document provides the purpose and method of use of all external TSF interfaces and completely represents the TSF.
ADV_HLD.2	This document describes the high level design. It contains a representation of the TSF in terms of subsystems, identifying the TSP-enforcing subsystems, and it describes the security functions. All subsystem interfaces are identified, and the externally-visible interfaces are noted. The purpose and method of use of all interfaces to the TSF subsystems are described.
ADV_RCR.1	This document describes the correspondence between the TOE security functions and the functional specification and the correspondence between the functional specification and the high-level design subsystems.
AGD_ADM.1	Guidance to administrators is effectively supported by the listed documentation for this requirement.
AGD_USR.1	Guidance to non-administrative users is effectively supported by the listed documentation for this requirement.

Component ID	Rationale
ALC_DVS.1	This document describes the development life cycle.
ATE_COV.2	This document describes the functional and vulnerability tests performed to cover the TOE SFRs and their results.
ATE_DPT.1	This document describes the functional and vulnerability tests performed to cover the TOE subsystems and their results.
ATE_FUN.1	This document describes the functional and vulnerability tests performed and their results.
ATE_IND.2	This document describes the functional and vulnerability tests performed and their results.
AVA_MSU.1	This document describes whether an administrator or user, with an understanding of the guidance documentation would be able to determine if the TOE is configured and operating in a manner that is secure.
AVA_SOF.1	This document includes a-strength of-function analysis to support the SOF basic claim. The analysis includes identifying the TOE password space and the probability of a password being compromised.
AVA_VLA.1	This document describes the vulnerability analysis performed and the results of the analysis.

Table 8-1 Assurance Measures

8.2.4.2 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is as follows:

- The TOE is consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market
- The TOE assurance also meets current constraints on widespread acceptance by expressing its claims against EAL3 from part 3 of the Common Criteria.

8.3 TOE Summary Specification Rationale

Section 6.3 demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.