Data Security Kit
(AR-FR1/AR-FR2/AR-FR3)

for the
Sharp Imager Family
(AR-287, AR-337, AR-407, and AR-507)

Security Target

Version 1.1g

PREPARED BY:

COMPUTER SCIENCES CORPORATION
7471 CANDLEWOOD ROAD
HANOVER, MD 21076

FOR
SHARP CORPORATION
SHARP DOCUMENT AND NETWORK SOLUTIONS GROUP
SHARP PLAZA, MAHWAH, NJ 07430-2135

Date	Version	Changes Made
September 19, 2000	0.1	Initial draft from CSC
November 6, 2000	0.2	Incorporate Sharp Comments
November 8, 2000	0.3	Incorporate ST Training Comments
December 28, 2000	0.4	Address Evaluator/Validator comments in DSK_EDR_002
January 3, 2001	0.5	Removed FPT_SEP.1 and FMT_SMR.1
January 19, 2001	0.6	Addressed Evaluator/Validator comments in DSK_EDR_002 and implemented changes per teleconference with Sharp.
February 1, 2001	0.7	Redefinition of the TOE and its boundaries and rewrites that are applicable to the changes.
February 9, 2001	0.8	Implemented comments from Evaluator/Validator.
February 15, 2001	0.8	Met with Evaluator and implemented comments. Version did not change because no EDR was created.
February 27, 2001	0.9	Removed policies from Section 3.3 and OE.RESIDUAL and all related references.
March 2, 2001	1.0	Added PIN change assumption, and version numbers of DSK chips.
March 6, 2001	1.1	Changed T.TAMPER and O.NO_TAMPER statements.

Table of Contents

List of Figures

List of Tables

1 SECURITY TARGET INTRODUCTION

1 This Chapter presents security target (ST) identification information and an overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

a) A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (Chapter 3, TOE Security Environment).

b) A set of security objectives and a set of security requirements to address the security problem (Chapters 4 and 5, Security Objectives and IT Security Requirements, respectively).

c) The IT security functions provided by the TOE that meet the set of requirements (Chapter 6, TOE Summary Specification).

2 The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex C, and Part 3, Chapter 5.

1.1 ST and TOE Identification

3 This section provides information needed to identify and control this ST and its Target of Evaluation (TOE). This ST targets Evaluation Assurance Level (EAL)2.

ST Title:	Sharp Corporation Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507) Security Target
ST Version:	1.1
Publication Date:	March 6, 2001
Authors:	Joan Wallace and Carl Souba of Computer Sciences Corporation
TOE Identification:	Sharp Corporation Data Security Kit (AR-FR1, AR-FR2, and AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507)
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (also known as ISO 15408)
ST Evaluator:	Computer Sciences Corporation (CSC)
Keywords:	Sharp, Sharp Corporation, Sharp Imager Family, AR-287, AR-337, AR-407, and AR-507, copy services, print services, scan services, object reuse, residual information protection, AR-FR1, AR-FR2, AR-FR3

1.2 References

4 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 August 1999, version 2.1, CCIMB-99-031.

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, version 2.1, CCIMB-99-032.

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, version 2.1, CCIMB-99-033.

[CEM_PART1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and General Model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Methodology for Information Technology Security Evaluation – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

1.3 Conventions, Terminology, and Acronyms

5 This section identifies the formatting conventions used to convey additional information and terminology. It also defines terminology and the meanings of acronyms used throughout this ST.

1.3.1 Conventions

6 This section describes the conventions used to denote Common Criteria (CC) operations on security functional components and to distinguish text with special meaning. The notation, formatting, and conventions used in this ST are largely consistent with those used in the CC. Selected presentation choices are discussed here.

7 The CC allows several operations to be performed on security functional components; *assignment*, *refinement*, *selection*, and *iteration* as defined in paragraph 2.1.4 of Part 2 of the CC are:

a) The *assignment* operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets [assignment_value(s)] indicates an assignment.

b) The *refinement* operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.

c) The *selection* operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text.*

d) *Iterated* functional components are given unique identifiers by appending to the component name, short name, and functional element name from the CC an iteration number inside parenthesis, i.e., FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2).

e) Plain *italicized text* is used to emphasize text.

1.3.2 Terminology

8 In the CC, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions:

User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Human user	Any person who interacts with the TOE.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Identity	A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Authentication data	Information used to verify the claimed identity of a user.
Object	An entity within the TOE Security Function (TSF1) Scope of Control (TSC2) that contains or receives information and upon which subjects perform operations.
Subject	An entity within the TSC that causes operations to be performed.
Authorized User	A user who may, in accordance with the TOE Security Policy (TSP3), perform an operation.
Security Functional Components	Express security requirements intended to counter threats in the assumed operating environment of the TOE.

9 The following terminology is specific to this ST.

Unauthorized User	An unauthenticated entity that interacts with the TOE Security Function (TSF) in a benign or malicious manner.

As defined in the CC, Part 1, version 2.1:
1 TSF - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
2 TSC - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
3 TSP – A set of rules that regulate how assets are managed, protected and distributed within a TOE.

Latent Image Data	Residual information remaining on the hard disk drive when a copy/print/scan job is completed, cancelled, or interrupted.
Key Operator	An authorized user who manages the Sharp Corporation Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507).
Imager Data	Information on the hard disk drive created by the copy/print/scan process. (In this document, the term imager is used interchangeably with the term copier.)
DSK	Refers to the Data Security Kit for Sharp Imager Family AR-287, AR337, AR-407, and AR-507, exclusively.

1.3.3 Acronyms

10 The following acronyms are used in this Security Target:

ACRONYM	DEFINITION
AUT	Authentication
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
DSK	Data Security Kit
EAL	Evaluation Assurance Level
EDR	Evaluation Discovery Report
FDP	User Data Protection CC Class
FIA	Identification and Authentication CC Class
FMT	Security Management CC Class
FPT	Protection of Security Functions
FSP	Functional Specification
HDD	Hard Disk Drive
HLD	High Level Design
ICU	Image Control Unit
ISO	International Standards Organization
ISO 15408	Common Criteria 2.1 ISO Standard
IT	Information Technology
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
MOF	Management of Functions
MTD	Management of TSF Data
NT	New Technology
OPE	Operation Panel Interface
OSP	Organization Security Policy

ACRONYM	DEFINITION
PCU	Process Control Unit
PP	Protection Profile
ROM	Read Only Memory
RVM	Reference Mediation
SAR	Security Assurance Requirement
SEP	Domain Separation
SFP	Security Function Policy
SFR	Security Functional Requirement
SM	Security Management
SMR	Security Management Roles
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UAU	User Authentication
UDP	User Data Protection

1.4 Security Target Overview

11 The TOE is the hard disk drive (HDD)-erase feature of the Data Security Kit (DSK) for the Sharp Corporation Imager Family, (AR-287, AR-337, AR-407, and AR-507) digital copier. The TOE includes the Image Control Unit (ICU) and the hard disk drive. The DSK is a factory- or field-installed Read Only Memory (ROM) security enhancement to the Sharp AR-287, AR-337, AR-407, and AR-507 digital image processing copiers. (Data Security Kit, AR-FR1 is for AR-287/337 copiers, AR-FR2 is for the AR-407 copier, and AR-FR3 is for the AR-507 copier). These copiers buffer document data on a HDD. The threats exist that this buffered data could be disclosed through subsequent print/scan/copier jobs, or an unauthorized user could access the document data buffered on the HDD. Although accessing the buffered data is not a trivial task, skilled individuals could acquire or attempt to acquire valuable information in the form of latent image data residing on the HDD.

12 These threats are mitigated through the installation of the DSK and implementation of its HDD-erase function. The HDD-erase function uses a random number generator on the ICU to generate random data, which overwrites the sections of the HDD where data was stored prior to final output.

13 A summary of the HDD-erase security features can be found in Section 2, TOE Description. A detailed description of the HDD-erase security features can be found in Section 6, TOE Summary Specification.

1.5 Common Criteria Conformance Claim

14 This ST conforms to Part 2 and Part 3 of the CC, Version 2.1.

2 TOE DESCRIPTION

15 This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

16 The DSK is a factory- or field-installed ROM upgrade for the Sharp AR-287/337/407/507 family of digital image processing copiers. The DSK product adds the HDD-erase functionality which provides the following TOE security functions (TSF):

a) Protection of Security Function (TSF_FPT)

b) User Data Protection (TSF_UDP)

17 The IT environment provides the following security functions:

a) Authentication (TSF_AUT)

b) Security Management (TSF_SM)

18 The DSK is a firmware enhancement to the digital image processor copiers in the form of ROMs. The architectural design of the copiers provide physical separation (TSF_FPT) from the IT environment. The Sharp AR-287/337/407/507 digital image processing copiers document data is buffered on a HDD. The TOE provides the HDD-erase function for user data protection (TSF_UDP). With automatic HDD-erase enabled, after the completion of any multi-functional printer operation, random data is written over the hard disk areas used to temporarily store document data. During that time, usually a second or less, a message is displayed on the operator panel that the HDD data is being cleared and no other operations are available. The Key Operator enables or disables the automatic HDD-erase function.

19 The DSK also allows the Key Operator to manually clear the entire HDD. For example, on occasions when it is necessary to remove a HDD, the Key Operator can manually invoke the DSK HDD-erase function before removing the drive to mitigate the risk that residual document data might fall into the wrong hands. This function would also be used in the case of loss of power. When power is dropped from the copier, any data currently on the HDD remains. After a successful power up, the Key Operator must manually invoke the HDD-erase function to ensure that all residual data (prior to loss of power) is overwritten (erased).

20 The authentication (TSF_AUT) and security management (TSF_SM) security functions are provided by the Operation Panel Interface (OPE) in the IT environment.

21 Figure 1 depicts the HDD-erase security function concept.

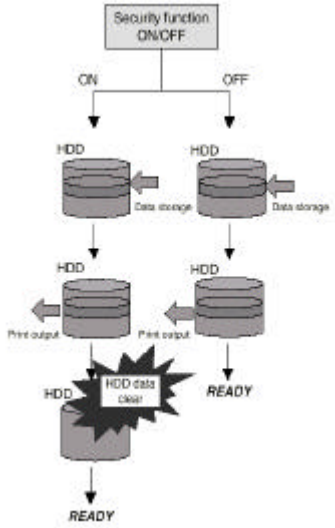

Figure 1: Sharp HDD-Erase Concept

2.2 Scope and Boundary of the Evaluated Configuration

22 This section provides a general description of the TOE physical and logical scope and boundaries. Figure 2 depicts the TOE physical and logical boundaries in relation to the DSK product.

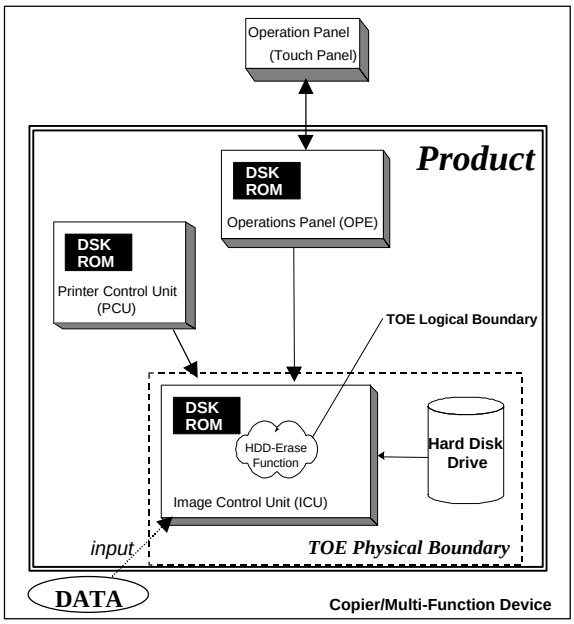

Figure 2: TOE Boundaries

2.2.1 Physical Scope and Boundary

23 The DSK is a firmware upgrade to existing ROMs on three of the copier's circuit boards. Each DSK consists of a set of three replacement ROMs, one each for the Process Control Unit (PCU), Image Control Unit (ICU) and Operation Panel Interface (OPE) circuit boards. The evaluated version of the PCU ROM is 2.30; the evaluated version of the ICU ROM is 2.33, and the evaluated version of the OPE ROM is 2.33. The DSK ROM on the ICU, the ICU circuit board, and the HDD comprise the TOE physical boundary. The other two DSK ROMs and their associated circuit boards and interfaces to the TOE provide the IT environment.

24 The ICU provides all of the HDD-erase functionality. The OPE and PCU DSK ROMs have no TOE security functionality. They are part of the DSK because they are keyed together for machine timing purposes and must be replaced simultaneously to ensure proper machine timing synchronization (e.g., paper movement).

25 As part of the IT environment, the OPE provides the TSF_AUT security function for the HDD-erase feature. The PCU and OPE do not contain any HDD-erase function code.

26 Table 1 identifies the TOE physical components.

Table 1: TOE Physical Components

Component	Description
ICU	Image Control Unit circuit board which interfaces with the HDD
ICU DSK ROM	ROM containing the firmware upgrade for HDD-erase functionality
HDD	Hard disk drive

2.2.2 Logical Scope and Boundary

27 The TOE logical boundary is the HDD-erase function on the ICU circuit board. The OPE ROM displays, on the Operator Panel, all of the liquid crystal display (LCD) screens associated with the HDD-erase function and provides a means for the Key Operator to activate or deactivate the automatic HDD-erase function or to manually invoke the HDD-erase function. Only users who are assigned as Key Operators and authenticated (via a personal identification number (PIN)) can activate/deactivate this security feature. Any user can utilize the other non-security-related features/functions of the copier without authentication.

28 The TOE provides the following security features:

a) **User Data Protection (UDP):** The TSF_UDP security mechanism protects information produced by a prior subject from disclosure to another subject or object by over writing data with random data on demand or automatically after every copy/scan/print event.

b) **Protection of Security Functions (FPT):** The TSF_FPT security mechanism ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed, and that the TSF maintains a security domain for its own execution that protects it from interference and tampering by unauthorized users.

29 The IT environment provides the following security features:

a) **Authentication (AUT):** The TOE utilizes the OPE software module security mechanisms to provide authentication functionality through the process of the Key Operator properly entering a 5-digit PIN before access to Key Operator functions is allowed. The default PIN must be changed by the Key Operator after installation is complete.

b) **Security Management (SM)**: The TSF_SM utilizes the OPE software module security mechanisms to allow only Key Operators the capability to enable or disable the automatic HDD-erase function or to manually clear the HDD at the end of a copy/scan/print job. The default setting is disabled.

3 TOE SECURITY ENVIRONMENT

3.1 Secure Usage Assumptions

30 This section describes the security aspects of the intended environment for the evaluated TOE. This includes information about the physical, personnel, procedural, connectivity, and functional aspects of the environment.

31 The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user/Key Operator guidance. The following specific conditions are assumed to exist in an environment where this TOE is employed.

3.1.1 Environment Assumptions

32 The environmental assumptions delineated in Table 2 are required to ensure the security of the TOE:

Table 2: Environmental Assumptions

Assumption	Description
A.HW_CORRECT	The security functionality within the TOE IT environment performs as documented for Sharp AR-287/337/407/507 digital image processing copiers.
A.INSTALL	The TOE hardware and software have been delivered, installed, and setup in accordance with documented delivery and installation/setup procedures.
A.MANAGE	There will be one or more competent Key Operator(s) assigned to manage the TOE and the security of the information it contains.
A.NO_EVIL_ADM	The Key Operator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Key Operator documentation.
A.PROCEDURE	Procedures exist for granting Key Operator(s) access to the TSF.
A.CHANGE_KOC	Key Operator's Code is changed at least every sixty (60) days.

3.2 Threats

33 Table 3 identifies the threats to the TOE. Mitigation to the threats is through the objectives identified in Section 4, Security Objectives.

Table 3: Threats to the TOE

Threat	Description
T.RESIDUAL	During the course of performing an authorized copy/print/scan job, a user may be the recipient of residual information remaining on the HDD from a previous copy/print/scan job.
T.TAMPER	An unauthorized user may tamper with the TOE to alter the HDD erase functionality; i.e., make the TOE appear to over write data on the HDD (erase HDD data), while in fact data is not being over written on the HDD.

3.3 Organizational Security Policies

34 No Organizational Security Policies (OSPs) are identified for the TOE.

4 SECURITY OBJECTIVES

35 The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the environment.

4.1 Security Objectives for the TOE

36 This section identifies and describes the security objectives of the TOE.

37 The TOE accomplishes the security objectives defined in Table 4.

Table 4: Security Objectives for the TOE

Objectives	Description
O.RESIDUAL	Data from one user process must not become available to any other user process.
O.NO_TAMPER	The TOE must operate in a separate domain that protects it from interference and tampering by unauthorized users.

4.2 Security Objectives for the Environment

38 The environment accomplishes the security objectives delineated in Table 5.

Table 5: Security Objectives for the Environment

Objectives	Description
OE.CORRECT	The security functionality within the environment must perform as documented for Sharp AR-287/337/407/507 digital image processing copiers.
OE.MANAGE	Only authorized Key Operators must be able to exercise security management functions provided by the TSF.

5 IT SECURITY REQUIREMENTS

39 This section defines the IT security requirements that shall be satisfied by the TOE or its environment:

40 The CC divides TOE security requirements into two categories:

- Security functional requirements (SFRs) (such as, identification and authentication, security management, and user data protection) that the TOE and the supporting evidence need to satisfy to meet the security objectives of the TOE.
- Security assurance requirements (SARs) that provide grounds for confidence that the TOE and its supporting IT environment meet its security objectives (e.g., configuration management, testing, and vulnerability assessment).

41 These requirements are discussed separately within the following subsections.

5.1 TOE Security Functional Requirements

42 The TOE satisfies the SFRs delineated in Table 6. The rest of this section contains a description of each component and any related dependencies.

Table 6: TOE Security Functional Requirements

Functional Component ID	Functional Component Name
Protection of Security Functions (TSF_PT)	
FPT_RVM.1	Non-bypassibility of the TSP
FPT_SEP.1	TSF Domain Separation
User Data Protection (TSF_UDP)	
FDP_RIP.1	Subset Residual Information Protection

5.1.1 Class FPT: Protection of TSF

43 FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components

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

Dependencies: No dependencies

44 FPT_SEP.1 TSF Domain Separation

Hierarchical to: No other components

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

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

Dependencies: No dependencies

5.1.2 Class FDP: User Data Protection

45 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: [end of a user job].

Dependencies: No dependencies

5.2 TOE Security Assurance Requirements

46 Table 7 identifies the security assurance components drawn from CC Part 3 Security Assurance Requirements EAL2. The rest of this section delineates the Developer and Evaluator action elements and the content and presentation evidence elements for each assurance component.

Table 7: EAL2 Assurance Requirements

Assurance Component ID	Assurance Component Name	Dependencies
ACM_CAP.2	Configuration items	None
ADO_DEL.1	Delivery procedures	None
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1
ADV_FSP.1	Informal functional specification	ADV_RCR.1
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1
ADV_RCR.1	Informal correspondence demonstration	None
AGD_ADM.1	Administrator guidance	ADV_FSP.1
AGD_USR.1	User guidance	ADV_FSP.1
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1

Assurance Component ID	Assurance Component Name	Dependencies
ATE_FUN.1	Functional testing	None
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ATE_HLD.1 AGD_ADM.1, AGD_USR.1

47 **ACM_CAP.2 Configuration items**

Developer action elements:

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

48 **ADO_DEL.1 Delivery procedures**

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

49 **ADO_IGS.1 Installation, generation, and start-up procedures**

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

50 **ADV_FSP.1 Informal functional specification**

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

51 **ADV_HLD.1 Descriptive high-level design**

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

52 **ADV_RCR.1 Informal correspondence demonstration**

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

53 **AGD_ADM.1 Administrator guidance**

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to

be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

54 **AGD_USR.1 User guidance**

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

55 **ATE_COV.1 Evidence of coverage**

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

56 **ATE_FUN.1 Functional testing**

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

57 **ATE_IND.2 Independent testing – sample**

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

58 **AVA_SOF.1 Strength of TOE security function evaluation**

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

59 **AVA_VLA.1 Developer vulnerability analysis**

Developer action elements:

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.1.1C The documentation shall show, for all identified vulnerabilities, including those identified in Appendix A of ALFPP v1.c, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.3 Security Requirements for the IT Environment

60 The IT environment satisfies the SFRs delineated in Table 8. However, environmental SFRs fall outside the scope of this evaluation. The rest of this section contains a description of each component and any related dependencies.

Table 8: IT Environment Security Functional Requirements

Functional Component ID	Functional Component Name
Identification and Authentication (TSF_AUT)	
FIA_UAU.2	User Authentication before any Action

Functional Component ID	Functional Component Name
FIA_UAU.7	Protected Authentication Feedback
Security Management (TSF_SM)	
FMT_MOF.1 (1)	Management of Security Functions Behavior (1)
FMT_MOF.1 (2)	Management of Security Functions Behavior (2)

5.3.1 Class FIA: Identification and Authentication

61 FIA_UAU.2 User Authentication Before Any Action

Hierarchical to: FIA_UAU.1 Timing of Authentication

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

Dependencies: FIA_UID.1 Timing of Identification

62 FIA_UAU.7 Protected Authentication Feedback

Hierarchical to: No other components

FIA_UAU.7.1 The TSF shall provide only [obscured feedback] to the **Key Operator** while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of Authentication

5.3.2 Class FMT: Security Management

63 FMT_MOF.1 (1) Management of Security Functions Behavior (1)

Hierarchical to: No other components

FMT_MOF.1.1(1) The TSF shall restrict the ability to *disable, enable, or* ***manually invoke*** the functions [associated with the Security Mode SFP] to [the Key Operator].

Dependencies: FMT_SMR.1 Security Roles

64 FMT_MOF.1 (2) Management of Security Functions Behavior (2)

Hierarchical to: No other components

FMT_MOF.1.1(2) The TSF shall restrict the ability to *determine the behavior of* the functions [

a) end of job cancel,

b) memory full, or

c) manually pressing the “CLEAR ALL HDD-DATA” button]

to [the Key Operator].

Dependencies: FMT_SMR.1 Security Roles

5.4 Explicitly Stated Requirements for the TOE

65 This ST does not contain explicitly stated requirements for the TOE. All SFRs have been drawn from the CC.

5.5 SFRs With SOF Declarations

66 The overall Strength of Function (SOF) claim for the TOE is SOF-basic.

67 FIA_UAU.2: The authentication mechanism, which is allocated to the IT evnironment, has a PIN space of 10^5.

68

6 TOE SUMMARY SPECIFICATION

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

6.1 TOE Security Functions

70 This section presents the security functions performed by the TOE to satisfy the identified SFRs in Section 5.1.1. Traceability to SFRs is also provided.

6.1.1 Protection of the TSF (TSF_FPT)

71 The architecture of the copier maintains a security domain for TOE execution that is protected from interference and tampering by untrusted subjects. The copier is a dedicated machine that provides copy/print/scan functionality as defined by the firmware contained in the copier. The TOE function is firmware confined to a circuit board that can only be accessed by disassembling the machine. All firmware, when executed, is considered to be trusted subjects. The copier does not have the capability to execute other software/firmware.

72 The TOE ensures that all TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. The TOE provides this functionality by being an integral part of the copier printing system. The DSK ICU ROM chip adds functionality to the copier to determine HDD-erase configuration status, (i.e., if HDD-erase is set). This check and functionality is integrated into the printing system firmware and is always performed at the conclusion of any print/scan/copy job and can not be bypassed. While clearing data, the copier does not accept any other job. When the copier is not processing a current job, the Key Operator can direct the TOE to erase the HDD.

73 **Functional Requirements Satisfied:** FPT_SEP.1 and FPT_RVM.1.

6.1.2 User Data Protection (TSF_UDP)

74 To mitigate the risk of data leakage, the TOE provides the HDD-erase function that can be configured to automatically clear data on the HDD after job completion. The HDD-erase function can be programmed to perform at the end of a print/scan/copy job, at the end of job cancel, when memory is full, or by manually pressing the “CLEAR ALL HDD-DATA” button.

75 The manual HDD-erase function overwrites the whole HDD, while the automatic function overwrites only the area of the HDD that was used to buffer the data from the last job processed. Random number patterns, (0s and 1s), are used in the overwrite process.

76 The following table lists the types of jobs to be cleared, the conditions under which the automatic HDD-erase is performed, and whether a message is displayed to the user during the activity.

Table 9: Automatic HDD-erase Programming Condition Options

Jobs to be cleared	Conditions for HDD-erase	Displaying message during erase activity
Copy	At the end of job	Yes
	At job cancellation (incl. case of memory full)	Yes
Interrupt copy	At the end of job	Yes
	At job cancellation (incl. case of memory full)	Yes
Printer	At the end of job	Yes
	At job cancellation (incl. case of memory full)	Yes
Scan/Print	At the end of job	Yes
	At job cancellation (incl. case of memory full)	Yes

6.1.2.1 Copy/Print/Scan

77 When the HDD-erase is invoked, in any mode, the HDD-erase message is displayed on the LCD operation panel. During clearing of HDD data, the print engine is in "not ready" status; each key is invalid (cancellation is disabled), and the user is not allowed to enter or run another job until the HDD-erase function completes.

6.1.2.2 Manual "CLEAR ALL HDD-DATA" Via Key Operation Programs

78 When the Key Operator presses the “CLEAR ALL HDD-DATA” key in the Key Operator programs on the operation panel, the TOE attempts to clear the whole HDD.

79 When the copier is in an idle state and the Key Operator selects “CLEAR ALL HDD-DATA”; a pop-up window for confirmation is displayed. The Key Operator selects ‘YES’ and then the following message is displayed:

HDD-DATA IS BEING CLEARED

80 There are three instances where the Key Operator cannot manually invoke the HDD-erase function:

1. While the machine is operating, selecting “CLEAR ALL HDD-DATA” results in the following display:

   CAN NOT CLEAR THE HDD-DATA NOW.
   SELECT IT AFTER CURRENT JOB IS COMPLETED.

2. While the machine is warming up, selecting “CLEAR ALL HDD-DATA” results in the following display:

CANNOT CLEAR THE HDD-DATA NOW.
SELECT IT AFTER WARMING UP IS COMPLETED.

3. When the machine is not ready, selecting "CLEAR ALL HDD-DATA" will result in the following display:

   CAN NOT CLEAR THE HDD-DATA NOW.
   SELECT THE COPIER MUST BE IN THE READY STATE.

81 **Functional Requirements Satisfied:** FDP_RIP.1.

6.2 Assurance Measures

82 The TOE satisfies CC EAL2 assurance requirements. This section identifies the Configuration Management, Delivery and Operation, Development, Guidance Documents, Testing, and Vulnerability Assessment Assurance Measures applied by Sharp to satisfy the CC EAL2 assurance requirements.

6.2.1 Configuration Management

83 The Configuration Management measures applied by Sharp include assigning a unique product identifier for each release of the TOE. Associated with this product identifier is a list of hardware, software, and firmware configuration items that comprise a single instance of the TOE. These configuration management measures are provided in the following Sharp documents:

1. Certificate of Registration, Certificate # JMI-0015, revision May 14, 1999 for Quality Management System compliant with IS)-9001:1994.

2. ISO-9001 Quality Manual, Eighth Edition, May 9, 1997.

3. Sharp Parts Guide, CODE 00ZAR507//PIE for Models AR-287; 337; 407; and 507.

84 **Assurance Requirements Satisfied:** ACM_CAP.2.

6.2.2 Delivery and Operation

85 Sharp provides Delivery and Operation documentation that describes what components are delivered with the TOE, guidance for initially installing it, and warnings about the importance of properly unpacking, installing and configuring the TOE. Sharp produces the product, delivers the product and installs the product. These delivery and operation measures are documented within the following Sharp documents:

1. ISO-9001 Quality Manual, Eighth Edition, May 9, 1997.

2. AR-FR1/AR-FR2/AR-FR-3 Installation Manual.

3. AR-FR1/AR-FR2/AR-FR-3 Data Security Kit Operation Manual.

86 **Assurance Requirements Satisfied:** ADO_DEL.1 and ADO_IGS.1.

6.2.3 Development

87 The Sharp Development documentation identifies the TOE security functions, identifies all externally visible TSF interfaces, describes the TSF behavior, describes the TOE in terms of subsystems, identifies TSF subsystem interfaces, identifies TSF subsystem externally visible interfaces, and provides a correspondence between that information and this ST. This development evidence is provided in the following Sharp documents:

1. Sharp Corporation, Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507), Functional Specification, Version 0.6

2. Sharp Corporation, Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507), High-level Design Document, Version 0.3

3. Sharp Corporation, Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507), Correspondence Evidence, Version 0.2

4. Data Security Mode Specification for Cougar 2000

5. Sharp Digital Copying Machine HDD Security Instructions (Spreadsheet)

6. Sharp Service Manual Digital Copier, Code 00ZAR507//A1E for Models: AR-235; 337; 407; and 507

7. Sharp Circuit Diagram CODE 00ZAR507//C1E, Digital Copier, Models: AR-287; AR-337; AR-407; AR-507

88 **Assurance Requirements Satisfied**: ADV_FSP.1, ADV_HLD.1, and ADV_RCR.1.

6.2.4 Guidance Documents

89 The Guidance Documents provided by Sharp include Installation, Administrator, and User Guidance that define the processes for unpacking, installing, and configuring the DSK. These guidance measures are provided in the following Sharp documents:

1. Sharp Model AR-287, AR-337, AR-407 Digital Copying Machine Operation Manual

2. Sharp Model AR-287, AR-337, AR-407 Digital Copying Machine Key Operator's Guide

3. Guide Model AR-507 Digital Copying Machine Operation Manual
4. Model AR-507 Digital Copying Machine Key Operator's Guide
5. AR-FR1/AR-FR2/AR-FR-3 Data Security Kit Operation Manual

90 **Assurance Requirements Satisfied:** AGD_ADM.1 and AGD_USR.1.

6.2.5 Tests

91 Sharp performed extensive testing of the DSK. The testing performed includes both functional and penetration testing to ensure that the DSK meets its design goals. These tests are described in the following Sharp documents:

1. Sharp Corporation, Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507), Vulnerability Assessment, Version 0.3
2. C2000 Security Function Check (Functional Test Plans)
3. OnTrack Test Results of HDD Erase function
4. Email dated January 9, 2001 and last updated February 27, 2001 from Cliff Quiroga of Sharp Corporation
5. The evaluator will further test the TOE to ensure that the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements.

92 **Assurance Requirements Satisfied**: ATE_COV.1, ATE_FUN.1, and ATE_IND.2.

6.2.6 Vulnerability Assessment

93 As part of the design and testing process, Sharp conducted a Vulnerability Analysis of the DSK. The goal of the analysis was to identify any obvious weaknesses that could be exploited by an attack. The results of the vulnerability analysis is described in the following Sharp document:

1. Sharp Corporation, Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507), Vulnerability Analysis, Version 0.3

94 **Assurance Requirements Satisfied:** AVA_SOF.1 and AVA_VLA.1.

7 PROTECTION PROFILE (PP) CLAIMS

95 The TOE does not claim conformance to a PP.

8 RATIONALE

96 This section demonstrates the completeness and consistency of this ST.

- *Traceability:* The security objectives for the TOE and its environment are explained in terms of threats countered and assumptions met. The SFRs are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following:
  - security objectives to threats encountered
  - environmental objectives to assumptions met
  - SFRs to objectives met
- *Assurance Level:* A justification is provided for selecting an EAL2 level of assurance for this ST.
- *SOF:* A rationale is provided for the SOF level chosen for this ST.
- *Dependencies:* A mapping is provided as evidence that all dependencies are met.

8.1 Security Objectives Rationale

97 This section provides evidence that at least one assumption or threat addresses each security objective. A justification as to why the security objective is suitable to counter the threat or cover the assumption is also provided.

98 **O.RESIDUAL** *Residual data on the hard disk drive from one user process must not become available to any other user process.*

99 This objective works to counter the T.RESIDUAL threat by enabling the HDD-erase function to be automatically performed after every copy/print/scan job, and cancelled copy/print/scan jobs, and manually invoked when necessary. The HDD-erase function overwrites any residual data with random data, leaving the residual data virtually unreadable.

100 **O.NO_TAMPER** *The TOE must operate in a separate domain that protects it from interference and tampering from unauthorized users.*

101 This security objective counters the T.TAMPER threat because the TOE is physically located internal to the copier and cannot be physically accessed without the proper tools. Users, even Key Operators, cannot introduce code to affect the TOE.

102 **OE.MANAGE** *Only authorized Key Operators must be able to exercise management functions provided by the TSF.*

103 This security objective is met by the A.MANAGE, A.NO_EVIL_ADM, A.CHANGE_KOC and A.PROCEDURE environmental assumptions. They acknowledge the need for competent Key Operators to manage the TOE, and that the Key Operators will not be careless, willfully negligent, or hostile. They also call for the existence and implementation of procedures for granting Key Operators access to the TOE and that the Key Operator code is changed at least every sixty (60) days.

104 **OE.CORRECT** *The security functionality within the TOE IT environment performs as documented for Sharp AR-287/337/407/507 digital image processing copiers.*

105 This security objective is met by the A.HW_CORRECT and A.INSTALL environmental assumptions because they acknowledge that the security functionality exists within the TOE IT environment and must perform as documented for Sharp AR-287/337/407/507 to implement established procedures. This includes the aspect that the TOE hardware and software have been delivered and setup in accordance with documented procedures.

Table 10: Objective Mappings to Threats and Assumptions

OBJECTIVE	THREATS and ASSUMPTIONS
O.RESIDUAL	T.RESIDUAL
O.NO_TAMPER	T.TAMPER
OE.MANAGE	A.MANAGE, A.NO_EVIL_ADM, A.PROCEDURE, A.CHANGE.KOC
OE.CORRECT	A.HW_CORRECT, A.INSTALL

8.2 Security Requirements Rationale

106 This section provides evidence that demonstrates that the security objectives for the TOE and the IT environment are satisfied by the security requirements.

107 These mappings demonstrate that all TOE security requirements can be traced back to one or more TOE security objective(s), and all TOE security objectives are supported by at least one security requirement.

8.2.1 Rationale For TOE Security Requirements

108 This section provides evidence demonstrating that the security objectives of the TOE are satisfied by the security requirements. The following paragraphs provide the security requirement to security objective mapping and a rationale to justify the mapping.

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

110 This SFR ensures that information contained on the HDD is not inadvertently disclosed. This SFR traces back to and aids in meeting the following objective: O.RESIDUAL.

111 **FPT_RVM.1 Non-bypassability of the TSP**

112 This SFR ensures the underlying security enforcement functions of the TOE are called, are activated, and are successful before the scope of control expands to include the TOE security functionality. This SFR traces back to and aids in meeting the following objectives: O.NO_TAMPER.

113 **FPT_SEP.1 TSF Domain Separation**

114 This SFR ensures that the TSF has a domain of execution that is separate from, and that cannot be violated by, unauthorized users. This SFR traces back to and aids in meeting the following objective: O.NO_TAMPER.

Table 11: TOE SFR Mapping to Objectives

	O.RESIDUAL	O.NO_TAMPER
(FDP_RIP.1) Subset Residual Information Protection	X	
(FPT_RVM.1) Non-bypassability of the TSP		X
(FPT_SEP.1) TSF Domain Separation		X

8.2.2 Rationale For IT Environment Security Requirements

115 **FIA_UAU.2 User Authentication Before Any Action**

116 This SFR ensures that Key Operators are authenticated before accessing the security functionality of the TOE. This SFR traces back to and aids in meeting the following objective: OE.MANAGE.

117 **FIA_UAU.7 Protected Authentication Feedback**

118 This SFR ensures that only obscured feedback generated by the authentication process is provided to Key Operators before successful authentication. This SFR traces back to and aids in meeting the following objective: OE.MANAGE.

119 **FMT_MOF.1 (1) Management of Security Functions Behavior (1)**

120 This SFR ensures that only Key Operators have the capability to enable, disable, or manually invoke the Security Mode SFP. This SFR traces back and aids in meeting the following objective: OE.MANAGE.

121 **FMT_MOF.1 (2) Management of Security Functions Behavior (2)**

122 This SFR ensures that only Key Operators have the capability to determine the behavior of the Security Mode SFP. This SFR traces back and aids in meeting the following objective: OE.MANAGE.

Table 12: IT Environment SFR Mapping to Objectives

	OE.MANAGE
(FIA_UAU.2) User Authentication before any Action	X
(FIA_UAU.7) Protected Authentication Feedback	X
(FMT_MOF.1 (1)) Management of Security Functions Behavior (1)	X
(FMT_MOF.1 (2)) Management of Security Functions Behavior (2)	X

8.3 Rationale For Assurance Level

123 This ST has been developed for Sharp AR-287/337/407/507 digital image processing copiers incorporating a DSK. The TOE environment will be exposed to a low level of risk because the TOE is internal to the copier and agents cannot physically access the TOE without disassembling the machine. Agents have no means of infiltrating the TOE with code to effect a change. As such, the Evaluation Assurance Level 2 is appropriate.

8.4 Rationale For TOE Summary Specification

124 This section demonstrates that the TSFs and Assurance Measures meet the SFRs.

125 The specified TSFs work together to satisfy the TOE SFRs. Table 13 provides a mapping of SFRs to the TSFs to show that each SFR is captured within a security function.

Table 13: Mapping of SFRs to Security Functions

TOE Security Function	Security Functional Requirement	Security Functional Requirement Name
User Data Protection (TSF_UDP)	FDP_RIP.1	Subset Residual Information Protection

TOE Security Function	Security Functional Requirement	Security Functional Requirement Name
Protection of Security Function (TSF_FPT)	FPT_RVM.1	Non-bypassibility of the TSP
	FPT_SEP.1	TSF Domain Separation

8.4.1 TOE Security Functions

126 The following paragraphs summarize which security functions implement specific functional requirements specified in Section 5.1.1, TOE Security Functional Requirements, as detailed in Section 6.1, TOE Security Functions.

127 SFR **FDP_RIP.1, Subset Residual Information Protection**, is implemented by the User Data Protection security function. Previous information is rendered unavailable upon resource deallocation because the HDD-erase function of the TOE overwrites the residual data on the HDD rendering it virtually unreadable. (TSF_UDP)

128 SFR **FPT_RVM.1, Non-bypassibility of the TSP**, is implemented by the TOE Protection of Security Functions function. An agent can not bypass TOE security enforcement unless the Key Operator PIN is known or the machine is disassembled. (TSF_FPT)

129 SFR **FPT_SEP.1, TSF Domain Separation**, is accomplished by the TOE Protection of Security Functions function. The architecture of the copier maintains a TSF domain and enforces separation between security domains of subjects in the TSC. (TSF_FPT)

8.4.2 TOE Assurance Requirements

130 Section 6.2 of this document identifies the Assurance Measures implemented by Sharp to satisfy the assurance requirements of EAL2 as delineated in the table in Annex B of the CC, Part 3. Table 14 maps the Assurance Requirements with the Assurance Measures as stated in Section 5.2.

Table 14: Assurance Measure Compliance Matrix

Assurance Measure	Configuration Management	Delivery and Operation	Development	Guidance	Test	Vulnerability Assessment
ACM_CAP.2	**X**					
ADO_DEL.1		**X**				
ADO_IGS.1		**X**				

Assurance Measure	Configuration Management	Delivery and Operation	Development	Guidance	Test	Vulnerability Assessment
ADV_FSP.1			**X**			
ADV_HLD.1			**X**			
ADV_RCR.1			**X**			
AGD_ADM.1				**X**		
AGD_USR.1				**X**		
ATE_COV.1					**X**	
ATE_FUN.1					**X**	
ATE_IND.2					**X**	
AVA_SOF.1						**X**
AVA_VLA.1						**X**

131 **ACM: Configuration Management**

132 Sharp documentation was reviewed to verify that Sharp has implemented a CM Plan that uniquely identifies each version of the TOE. Sharp also maintains a configuration list of each TOE version that describes the configuration items that comprise the TOE and the method used to uniquely identify them. It has been visually verified that the TOE is labeled with its reference number. These configuration management measures are provided in the following Sharp documents:

1. Certificate of Registration, Certificate # JMI-0015, revision May 14, 1999 for Quality Management System compliant with IS0-9001:1994.

2. ISO-9001 Quality Manual, Eighth Edition, May 9, 1997.

3. Sharp Parts Guide, CODE 00ZAR507//PIE for Models AR-287; 337; 407; and 507.

133 **ADO: Delivery and Operation**

134 Sharp satisfies the Delivery and Operation (ADO) assurance requirements because Sharp personnel are responsible for the DSK from development through delivery through installation. Only after complete delivery, installation, setup and configuration is the DSK responsibility transferred to the customer. Documentation that the Sharp personnel reference is listed below and found to be sufficient to ensure that the installation, generation, and start-up procedures will result in a secure configuration.

1. ISO-9001 Quality Manual, Eighth Edition, May 9, 1997.

2. AR-FR1/AR-FR2/AR-FR-3 Installation Manual.

3. AR-FR1/AR-FR2/AR-FR-3 Data Security Kit Operation Manual.

135 **ADV: Development**

136 The FSP identifies the TSF and its externally visible interfaces as being the interface to the OPE and the interface to the PCU. The FSP provides details of the effects, error messages and exceptions of each interface as being found in the DSK Key Operator's Guide, the DSK Machine Operation Manual, the DSK Installation Manual, and the C2000 Security Function Check document.

137 The DSK HLD describes the TSF in terms of four subsystems, the Monitor Subsystem, the HDD-erase Subsystem, and the Data Manipulation Subsystem. The HLD describes the security functionality of each subsystem, their interfaces, and which of those interfaces are externally visible.

138 The DSK RCR document provides a table showing the relationship between the Defined Security Function, SFRs, FSP Security Function, FSP Interfaces and the Rationale between the ST and FSP and the FSP and HLD. It also includes the relationships to the subsystems described in the HLD.

139 The following documents provide the evidence stated above:

1. Sharp Corporation, Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507), Functional Specification, Version 0.6

2. Sharp Corporation, Data Security Kit (AR-FR1/AR- FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507), High-level Design Document, Version 0.3

3. Sharp Corporation, Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507), Correspondence Evidence, Version 0.2

4. Data Security Mode Specification for Cougar 2000

5. Sharp Digital Copying Machine HDD Security Instructions (Spreadsheet)

6. Sharp Service Manual Digital Copier, Code 00ZAR507//A1E for Models: AR-235; 337; 407; and 507

7. Sharp Circuit Diagram CODE 00ZAR507//C1E, Digital Copier, Models: AR-287; AR-337; AR-407; AR-507

140 **AGD: Guidance Documents**

141 The Guidance documents listed below contain the information needed to satisfy the Guidance Document assurance requirements. The only type of administrator for the Sharp copiers is the Key Operator. These manuals describe the Key Operator security functions and how to implement them in a secure manner. The operator manuals also provide guidance for the proper secure operation of the copier.

1. Sharp Model AR-287, AR-337, AR-407 Digital Copying Machine Operation Manual
2. Sharp Model AR-287, AR-337, AR-407 Digital Copying Machine Key Operator's Guide
3. Guide Model AR-507 Digital Copying Machine Operation Manual
4. Model AR-507 Digital Copying Machine Key Operator's Guide
5. AR-FR1/AR-FR2/AR-FR-3 Data Security Kit Operation Manual

142 **ATE: Tests**

143 The documentation listed below contains satisfactory evidence that the TSF as described was successfully tested. The evaluator will also conduct further testing as well as reproduce the developer's test to ensure that the TSF operates as described.

1. Sharp Corporation, Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507), Vulnerability Assessment, Version 0.3
2. C2000 Security Function Check (Functional Test Plans)
3. OnTrack Test Results of HDD Erase function
4. Email dated January 9, 2001 with latest update of February 27, 2001 from Cliff Quiroga of Sharp Corporation
5. The evaluator will further test the TOE to ensure that the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements.

144 **AVA: Vulnerability Assessment**

145 Section 8.5.3 discusses strength of function of the TOE as SOF-basic because an attacker could not affect the TOE without the proper tools. Listed below is the Vulnerability Analysis document that addresses obvious weaknesses that could be exploited by an attack.

146 This document satisfies the Vulnerability Assessment (AVA) class of assurance requirements.

1. Sharp Corporation, Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for the Sharp Imager Family (AR-287, AR-337, AR-407, and AR-507), Vulnerability Analysis, Version 0.3

8.4.3 TOE SOF Claims

147 The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Sections 8.2.1 and 8.2.2 demonstrate that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The SOF-basic claim for the TOE applies because the TOE protects against an unskilled attacker with no special tools from accessing the TOE. The claim of SOF-basic ensures that the mechanism is resistant to a low attack potential because the TOE is completely internal to the copier and cannot be accessed by subjects.

8.5 Rationale For SFR and SAR Dependencies

148 Table 15 is a cross-reference of the functional components, their related dependencies, and whether the dependency was satisfied. As evidenced by Table 15, all of the dependencies have been satisfied with the exception of FIA_UID.1 and FMT_SMR.1. FIA_UID.1 states that certain TSF functions can be performed prior to being authenticated, but the TOE requires authentication prior to performing any TSF functions. FMT_SMR.1 requires identifying the different roles that the TSF recognizes. The TOE has no concept of roles. Once the Key Operator is authenticated, the TOE has an assumption of roles because only an authenticated individual can access the TSF of the TOE. Therefore, the satisfaction of FIA_UID.1 and FMT_SMR.1 is not applicable.

Table 15: SFR Dependencies Status

Functional Component ID	Functional Co nponent Name	Dependency (ies)	Satisfied
FDP_RIP.1	Subset Residual Information Protection	None	NA
FIA_UAU.2	User Authentication before any Action	FIA_UID.1	NO
FIA_UAU.7	Protected Authentication Feedback	FIA_UAU.1	YES
FMT_MOF.1 (1)	Management of Security Functions Behavior (1)	FMT_SMR.1	NO
FMT_MOF.1 (2)	Management of Security Functions Behavior (2)	FMT_SMR.1	NO
FPT_RVM.1	Non-bypassibility of the TSP	None	NA
FPT_SEP.1	TSF Domain Separation	None	NA

149 SAR dependencies identified in the CC have been met by this ST as shown in Table 16.

Table 16: EAL2 SAR Dependencies Satisfied

Assurance Component ID	Assurance Component Name	Dependencies	Satisfied
ACM_CAP.2	Configuration items	None	NA
ADO_DEL.1	Delivery procedures	None	NA
ADO_IGS.1	Installation, generation, and start-up procedures	AGD_ADM.1	YES
ADV_FSP.1	Informal functional specification	ADV_RCR.1	YES
ADV_HLD.1	Descriptive high-level design	ADV_FSP.1, ADV_RCR.1	YES
ADV_RCR.1	Informal correspondence demonstration	None	YES
AGD_ADM.1	Administrator guidance	ADV_FSP.1	YES
AGD_USR.1	User guidance	ADV_FSP.1	YES
ATE_COV.1	Evidence of coverage	ADV_FSP.1, ATE_FUN.1	YES
ATE_FUN.1	Functional testing	None	NA
ATE_IND.2	Independent testing-sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	YES
AVA_SOF.1	Strength of TOE security function evaluation	ADV_FSP.1, ADV_HLD.1	YES
AVA_VLA.1	Developer vulnerability analysis	ADV_FSP.1, ATE_HLD.1 AGD_ADM.1, AGD_USR.1	YES

8.6 Rationale for Explicitly Stated Requirements

150 This ST does not contain explicitly stated requirements.

8.7 Internal Consistency and Mutually Supportive Rationale

151 The set of security requirements provided in this ST form a mutually supportive and internally consistent whole for the following reasons:

a) The choice of security requirements is justified as shown in Sections 8.3 and 8.4. The choice of SFRs and SARs is based on the assumptions about the objectives for, and the threats to, the TOE and the security environment. This ST provides evidence that the security objectives counter threats to the TOE, and that physical, personnel, and procedural assumptions are satisfied by security objectives for the TOE environment.

b) The security functions of the TOE satisfy the SFRs as shown in Table 13. All SFR and SAR dependencies have been satisfied or rationalized as shown in Table 15 and Table 16 and described in Section 8.6.

c) The SARs are appropriate for the assurance level of EAL2 and are satisfied by the TOE as shown in Table 14. EAL2 was chosen to provide a basic level of independently assured security with the assumption that products used in these environments will meet the security needs of the environment.

d) The SFRs and SARs presented in Section 5 and justified in Sections 8.3 and 8.4 are internally consistent. There is no conflict between security functions, as described in Section 2 and Section 6, and the SARs to prevent satisfaction of all SFRs.

APPENDIX A:

ADDITIONAL UNEVALUATED OPTIONS

ADDITIONAL UNEVALUATED OPTIONS

152 The following is a list of additional options or products that could be used with the DSK, but as of the writing of this ST, they have not been evaluated. These options/products were not installed on the evaluated copier.

- **Secure Print Release; D-SP:** This NT server-based application complements the Data Security Kit by holding documents to be printed on the copiers in the network's secured NT print queue until the user arrives at the copier/printer and provides identification in the form of an ID card and PIN. Immediately after the job prints, the Data Security Kit clears the print job data from the copier's HDD.

- **Release Station; D-RS:** This computer-based application provides security control over the release of print jobs making it possible to manually deny printing of a particular job or delete it.

- **Enterprise Edition Accounting Server; D-EE:** D-EE is an NT Accounting server bundle that tracks all print and copy activity by user, by workgroup, or by device providing complete records on usage patterns. It can provide a network-based audit trail of print and copy activity.

- **Professional Edition Accounting Server; D-PE:** D-PE adds support for Macintosh computers and provides a charge back or client billing feature for the accounting server.

- **Security Suite; D-SS:** D-SS imposes digital fingerprints on printed documents that provide tool to trace their origin. A print document archive supported by the software can be used to recreate original documents from fragments using digital fingerprints.

- **Axis 7000 Scan Server for the Imager Series; AR-AX7000:** This accessory for the Imager series complements the Data Security Kit by providing NT and Mail Server authentication for scan to E-mail and scan to file applications providing an audit trail for copier scanning applications. XML support provides the option of adding text labels to scanned document images using the Axis 7000 keyboard; and lightweight directory access protocol (LDAP) that provides access to the E-mail server global directory for more efficient scan to E-mail. Documents that are scanned are also buffered on the copier hard drive and cleared by the Data Security Kit.

153 The optional network server-based products identified above can be used to complement the DSK by providing an audit trail indicating who used the copier/printer/scanner. The server-based software can also control the release of print jobs from the network until the person who initiated the print job is at the Sharp machine. This prevents the possibility of documents lying in an open output where they can be viewed by others. The ID card reader and PIN entry pad used in conjunction with the server-based applications can be used to identify individuals who use the copier/printer/scanner, and restrict access. The AR-AX7000 provides an authentication solution for scanning and document communication (E-Mail) applications.

154 The product, as evaluated, did not include any of the above-mentioned options/products. No claims are made in this ST regarding Data Security Kit functionality not included in this ST. It is therefore emphasized that *operating the TOE outside its evaluated configuration negates the security claims made in this ST*.