TOSHIBA

System Software
for
e-STUDIO352/452

Security Target

7 March 2006
Ver 2.1

This document is a translation of the security target written in Japanese, which has been evaluated and certified. The Japan Certification Body has reviewed and checked it.

TOSHIBA TEC CORPORATION

Table of Contents

1. SECURITY TARGET INTRODUCTION

This chapter describes security target (hereinafter referred to as "ST") identification information, overview of the ST, conformance to the Common Criteria for Information Technology Security Evaluation (hereinafter referred to as "CC"), terms, abbreviations, and trademarks and registered trademarks used in this document.

1.1 ST Identification

Information to identify this ST is as described below:

ST Title	:	System Software for e-STUDIO352/452 Security Target
ST Version	:	Ver1.3
Publication Date	:	7 March 2006
Authors of ST	:	Document Processing & Telecommunication Systems Company, Toshiba TEC Corporation
TOE Identification		
[Japanese]	:	System Software for e-STUDIO352/452 (in Japanese)
[English]	:	System Software for e-STUDIO352/452
TOE Version	:	V1.0
Authors of TOE	:	Document Processing & Telecommunication Systems Company, Toshiba TEC Corporation
Assurance Level	:	EAL3
Keywords	:	Digital multi function device, MFP, e-STUDIO, GP-1060, Data Delete Function, Data Overwrite, Toshiba TEC Corporation
CC Identification	:	Common Criteria for Information Technology Security Evaluation Version 2.1 CCIMB Interpretations (as of 01 December 2003)
Evaluation Methodology	:	Common Methodology for Information Technology Security Evaluation Version 1.0 CCIMB Interpretations (as of 01 December 2003)

1.2 ST Overview

This ST specifies the security functions of the System Software installed on the Toshiba TEC Corporation's digital multi function device, e-STUDIO352/452.

The e-STUDIO352/452 input a user document and output it in various formats (hereinafter referred to as "e-STUDIO General Functions").

The TOE is the System Software of the e-STUDIO352/452 having both the e-STUDIO General Functions and security functions.

The Data Delete Function, a security function of the TOE, provides the function which permanently erases user document data, deleted by the operation system's file delete function, from the hard disk drive of the e-STUDIO352/452 (hereinafter referred to as "HDD").
Note that "permanently erase" here means the user document data is deleted in an unrecoverable manner.

The Data Delete Function further provides the function which collectively and permanently erases all user document data from the HDD of the e-STUDIO352/452 before the HDD is disposed of or replaced. This function permanently erases all residual user document data in the HDD.

1.3 CC Conformance

This ST conforms to the following CC specifications:

- CC Version 2.1, Part 2 conformant
- CC Version 2.1, Part 3 conformant
- Assurance level: EAL 3 conformant
- There are no Protection Profiles (PPs) to which this ST is conformant.

1.4 Terms and Abbreviations

The following terms and abbreviations are used in this ST.

<CC-related abbreviations>

- CC Common Criteria
- EAL Evaluation Assurance Level
- PP Protection Profile
- ST Security Target
- TOE Target Of Evaluation
- SOF Strength Of Function
- TSF TOE Security Function
- TSP TOE Security Policy
- TSC TSF Scope of Control

<TOE-related terms and abbreviations>

- MFP — Multi Function Peripherals (Digital multi function device)
  A single multi-functional peripheral device which integrates several functions such as copy, print, and fax.
- e-STUDIO — MFPs where the TOE is installed, i.e., e-STUDIO352/452 (e-STUDIO352, and e-STUDIO452).
- HDD — Hard Disk Drive
- User document data — e-STUDIO user's document data, digitized utilizing the e-STUDIO General Functions. Note that data sent by a facsimile machine and received by the e-STUDIO using its standard fax function is not user document data of the e-STUDIO user but the data of a person who has sent it.
- e-Filing Box — A filing box where the e-STUDIO user stores his/her user document data. Such user document data is automatically deleted from the e-Filing Box after a specified effective period expires. There are two types of e-Filing Boxes, public box and private user box as described below:
  - Public box
    All users can access, edit, and print user document data stored in this box.
  - Private user box
    Every user can create his/her own user boxes, give each box a name, and assign a password to each of them.
    The user who created a private user box can access, edit, and print user document data in his/her own private user box.
    Note that the use of password does not contribute to the Data Delete Function which is the TOE security objective used as a preventive measure against potential threads to the TOE.
- Shared folder — e-STUDIO users can store and retrieve user document data in a shared folder. Such user document data is automatically deleted from the shared folder after a specified effective period expires.
- GP-1060 — A product installed in the e-STUDIO352/452 to enable the Data Delete Function, a security function of the System Software

1.5 Trademark Notice

- VxWorks is a registered trademark or trademark of Wind River Systems, Inc.
- All other product names mentioned in this ST may be trademarks or registered trademarks of their respective owners.

2. TOE DESCRIPTION

This chapter describes the product type, usage environment, product configuration, functions, and threads regarding the e-STUDIO352/452.

2.1 Product Type and Usage Environment

This ST defines four types of MFPs, e-STUDIO352, and e-STUDIO452, each having different print speed. The TOE is the common control software among them.

As shown in Figure 2.1 below, the e-STUDIO352/452 are used as a terminal to send/receive data to/from facsimiles, a terminal to send Email to Email servers, and a remote printer for remote PCs in network environments as well as they are installed in general offices as a standalone copier.

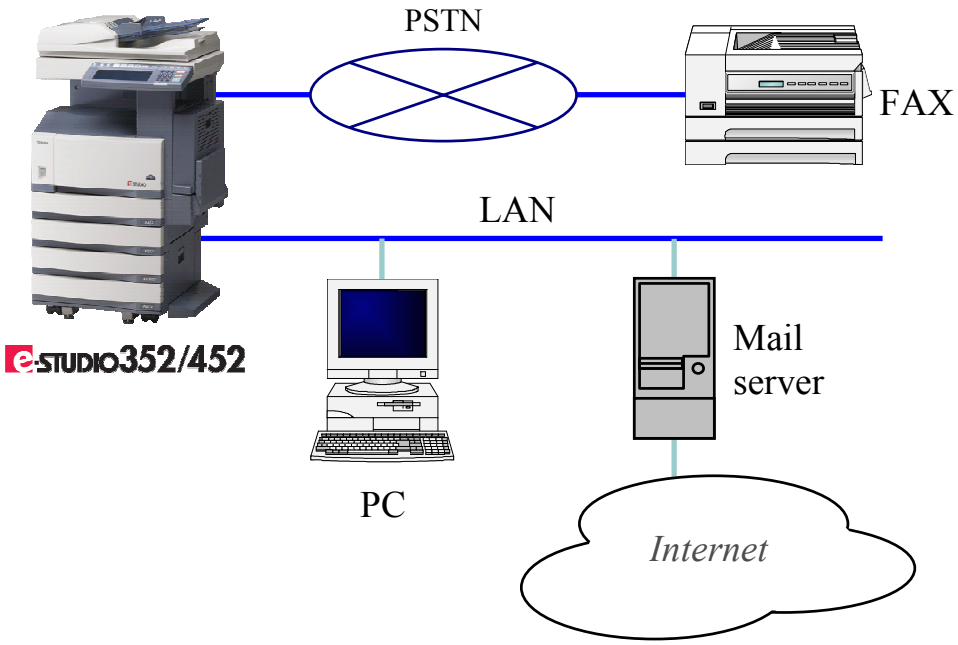

Figure 2.1 Use of the e-STUDIO in Network Environment

The MFP is a digital multi function device which inputs, processes, and outputs user documents. Its output processes are copy, print, scan, and fax reception and fax transmission. After each process completes, user document data is deleted by the file delete function provided by the operation system, except for the cases when the e-STUDIO user stores his/her user document data in an e-Filing Box or a shared folder in the HDD.

User document data stored in e-Filing Boxes in the HDD are managed by each e-STUDIO user based on importance and confidentiality of the user document data and deleted using the operation system's file delete function as necessary.

Actually, the operation system's file delete function only clears a file pointer in the FAT (File Allocation Table) managed by the operation system. This means, an entity of the user document data still exists in the HDD, while the user believes the user document data no longer exists there.

Under this condition, a thread exists because any attacker who has knowledge about OS tools may be able to directly access the HDD and recover the user document data deleted by the operation system's file delete function by reverse engineering the area where the applicable user document data is written.

The Data Delete Function, which is a TOE's security function, provides a function to permanently erase user document data deleted by the operation system's file delete function and a function to collectively and permanently erase residual user document data in the HDD before the HDD is disposed of or replaced.

Here, "permanently erase" means the user document data is deleted in an unrecoverable manner.

Also, residual user document data in e-Filing Boxes and shared folder of the HDD means any data still remains in the e-Filing Boxes and the shared folder, not having been deleted by the e-STUDIO users when the HDD will not be managed by the e-STUDIO users any longer, for example at the time of disposal or replacement of the HDD.

Note that the e-STUDIO's Data Delete Function becomes effective only when the GP-1060 is installed.

The following shows hardware and software configuration of the e-STUDIO.

Hardware Configuration	Specification
e-STUDIO352/452	e-STUDIO352 : 35 sheets/min. Copy/print speed on A4-size or e-STUDIO452 : 45 sheets/min. LETTER-size papers
GP-1060	USB interface

Table 2.1-1 e-STUDIO Hardware Configuration

Software Configuration	Function
System Software V1.0	System Software for controlling the e-STUDIO352/452
UI data (Optional languages) Japanese: V012.000 2 American English: V011.000 3 European English: V011.000 4 French: V011.000 6 Italian: V011.000 10 German: V012.000 7 Spanish: V011.000 11	Language data for each destination (nation)
VxWorks 5.5	OS

Table 2.1-2 e-STUDIO Software Configuration

2.2 Product Functions and TOE

The products, the e-STUDIO352/452 are special-purpose equipment having IT features and Data Delete Function implemented on the operation system (VxWorks). Here, the IT features are processes of copy, print, scan, fax transmission, fax reception, and deletion of data from an e-Filing Box (hereinafter collectively referred to as "e-STUDIO General Functions" as described in Section 1.2).

The TOE is software for the e-STUDIO352/452 which resides in the ROM of these models and conducts overall control on them.

The e-STUDIO352/452 start in normal mode where e-STUDIO users operate these models in ordinary cases.

In normal mode, the e-STUDIO General Functions and the security function in normal mode (Refer to Section 2.2.1.2.) are available.

Besides the normal mode, the e-STUDIO offers a self-diagnostic mode where service engineers perform maintenance services. When the e-STUDIO starts in this mode, the e-STUDIO General Functions and security function in normal mode are disabled. In self-diagnostic mode, only the security function in this mode (Refer to Section 2.2.2.2.) is available.

2.2.1 Features in Normal Mode and TOE

Figure 2.2.1 shows the configuration of the e-STUDIO352/452 in normal mode. User document data exist only in the work area of the HDD, specified e-Filing Boxes, and shared folder.

Overall System Software shown in Figure 2.2.1, excluding the operation system, is the TOE of this ST in normal mode.

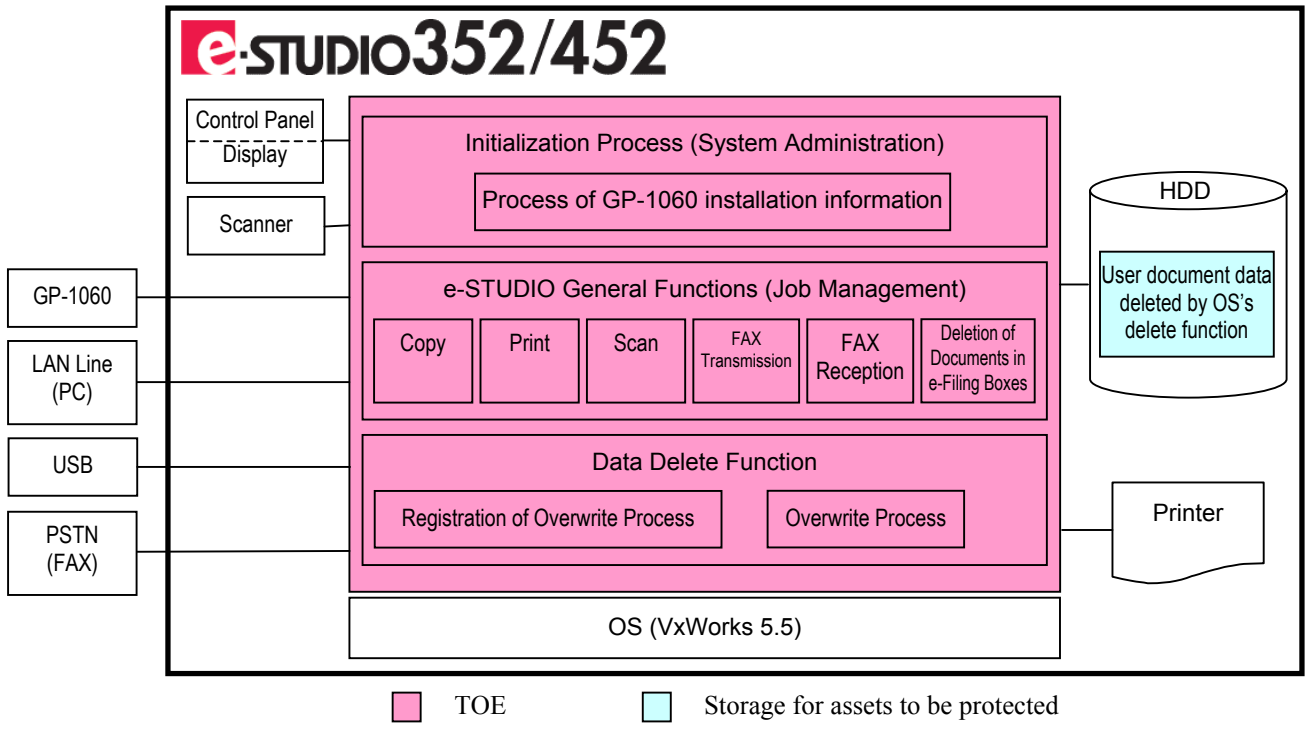

Figure 2.2.1 Product Configuration in Normal Mode

2.2.1.1 e-STUDIO General Functions in Normal Mode

(1) Process of GP-1060 Installation Information
This process checks whether or not the GP-1060 is installed.
In order to make the e-STUDIO users aware that the Data Delete Function is available, the TOE name and TOE version "SYS V1.0" are displayed next to the product name on the MFP's front cover and on the LCD display of the control panel.

(2) Copy process
When the START button is pressed with the copy function selected, this process scans user document data using

the scanner and writes the scanned data in the work area of the HDD.
Then, this process reads the user document data in the work area and performs both or either of the following processes:

- Outputs the user document data to the printer.
- Saves the user document data in an e-Filing Box or a shared folder in the HDD specified by the e-STUDIO user.

(3) Print process
This process receives user document data via a LAN line (PC) or a USB, or reads user document data in an e-Filing Box, and write the data in the work area of the HDD.
Then, this process reads the user document data in the work area and performs both or either of the following processes:

- Outputs the user document data to the printer.
- Saves the user document data in an e-Filing Box or a shared folder in the HDD specified by the e-STUDIO user.

(4) Scan process
When the START button is pressed while the SCAN button is being held down, this process scans user document data using the scanner and performs both or either of the following processes:

- Saves the user document data in an e-Filing Box or a shared folder in the HDD specified by the e-STUDIO user.
- Sends Email to a destination specified by the e-STUDIO user.

(5) Fax transmission process
When the START button is pressed while the FAX button is being held down, this process scans user document data using the scanner and writes the scanned data in the work area of the HDD.
Then, this process reads the user document data in the work area and sends the data to facsimile(s). The data can also be saved in a shared folder.

(6) Fax reception process
This process receives user document data from a facsimile and writes the data in the work area of the HDD.
Then, this process reads the user document data in the work area and performs both or either of the following processes:

- Outputs the user document data to the printer.
- Saves the user document data in an e-Filing Box or a shared folder in the HDD specified by the e-STUDIO user.

(7) Delete process of document in e-Filing Box and shared folder
This process deletes user document data which was saved in an e-Filing Box or a shared folder in the HDD, when commanded by the control panel or from a PC via a LAN line.

2.2.1.2 Security Functions in Normal Mode (Data Delete Function)

(1) Data Overwrite registration process

- After each process of the e-STUDIO General Functions described above, this process registers it with the trash box where user document data in the work area, deleted by the operation system's file delete function, is stored.
- During Process (7) of the e-STUDIO General Functions described above, this process registers it with the trash box where user document data which are stored in a e-Filing Box and a shared folder in the HDD, deleted by the operation system's file delete function, is stored.

(2) Data Overwrite process
This TOE checks if user document data has been registered with the trash box and if any, permanently erases it. The method used here is DoD5220.22-M of the US Department of Defense. While this process is being executed, the message "ERASING DATA" is displayed on the control panel.

2.2.2 Functions in Self-diagnostic Mode and TOE

Figure 2.2.2 shows the configuration of the e-STUDIO352/452 in self-diagnostic mode. Overall System Software shown in Figure 2.2.2, excluding the operation system, is the TOE of this ST in self-diagnostic mode.

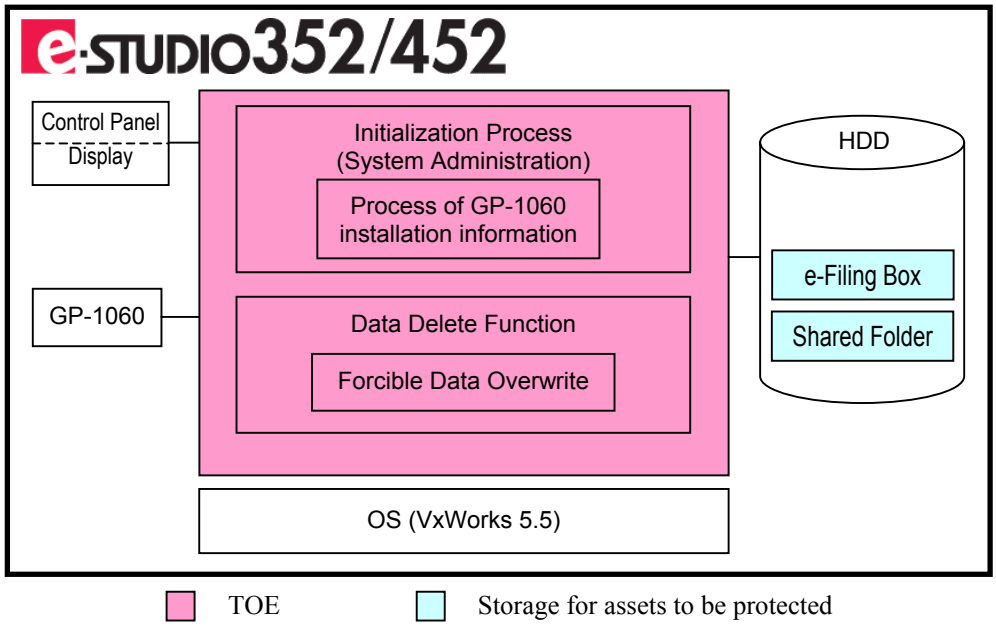

Figure 2.2.2 Product Configuration in Self-diagnostic Mode

2.2.2.1 e-STUDIO General Functions in Self-diagnostic Mode

- Process of GP-1060 Installation Information
  This process checks whether or not the GP-1060 is installed.
  In order to make the e-STUDIO users aware that the Data Delete Function is available, the TOE name and TOE version are displayed on the LCD display.

2.2.2.2 Security Functions in Self-diagnostic Mode

- Forcible Data Overwrite process
  When the TOE executes the forcible Data Overwrite process in self-diagnostic mode, it collectively and permanently erases all areas in the HDD where user document data are written. The method used here is DoD5220.22-M of the US Department of Defense.

2.3 TOE-related Personnel

The following describes personnel required for operating the TOE.

2.3.1 e-STUDIO Users

Users who utilize the e-STUDIO General Functions of the e-STUDIO352/452

2.3.2 e-STUDIO Administrators

Administrators make each setting of the TOE's General Functions (including copy, network, and fax settings) and ask service engineers to execute the forcible Data Overwrite function to the HDD. Note that they do not manage the TOE's security functions.

2.3.3 Service Engineers

Service engineers perform service maintenance operations such as installation of the e-STUDIO352/452 (including installation of the GP1060).
Upon request from the e-STUDIO administrator, the service engineer operates the TOE in self-diagnostic mode, then

executes the forcible Data Overwrite function to collectively and permanently erases all HDD areas of the e-STUDIO352/452 where user document data are stored.

2.4 Assets to be Protected

The assets to be protected by this TOE is an entity of residual user document data in the HDD after being deleted by the operation system's file delete function.

The user document data are deleted by the operation system's file delete function at the following timings:

- when a job completes,
- when a job is deleted,
- when a job is cancelled,
- when user document data stored is deleted, and
- when all files are deleted collectively.

* "Job" here means the e-STUDIO General Functions such as copy and print executed by the e-STUDIO352/452.
* Data sent by a facsimile machine and automatically received by the e-STUDIO using its standard fax function is not user document data of the e-STUDIO user but the data of a person who has sent it. Therefore, it is not an asset to be protected.
* User document data stored in e-Filing Boxes and a shared folder are no longer recognized as assets to be protected after such data's effective period expires.

3. TOE SECURITY ENVIRONMENT

This chapter describes the assumptions, threats, and organizational security policies for the TOE.

3.1 Assumptions

There are no assumptions.

3.2 Threats

The following are the potential threats to the e-STUDIO352/452.

- **T.TEMPDATA_ACCESS**
  By using off-the-shelf tools and by means of reverse engineering to the areas where residual user document data exists, a malicious e-STUDIO user or non-privileged user may attempt to recover or decode user document data, deleted from the HDD of the e-STUDIO352/452 by the operation system's file delete function.

- **T.STOREDATA_ACCESS**
  Using off-the-shelf tools, a malicious e-STUDIO user or non-privileged user may attempt to recover or decode the areas in the HDD of the e-STUDIO352/452 where user document data had existed and were deleted when all files were deleted collectively by the operation system's file delete function.

3.3 Organizational Security Policies

There are no organizational security policies for the TOE.

4. SECURITY OBJECTIVES

This chapter describes security objectives for the TOE and security objectives for the environment.

4.1 Security Objectives for the TOE

The following are the security objectives for the TOE.

- **O.TEMPDATA_OVERWRITE**
  The TOE must permanently erase the areas in the HDD of the e-STUDIO352/452, from which user document data were deleted, in order to prevent such areas from being recovered or decoded.

- **O.STOREDATA_OVERWRITE**
  The TOE must prevent the areas in the HDD of the e-STUDIO352/452, from which all files were deleted collectively, from being recovered or decoded.

4.2 Security Objectives for the Environment

The following are the security objective for the environment.

- **OE.OVERWRITE_COMPLETE**
  When collecting printout from the e-STUDIO352/452, e-STUDIO users must make sure that user document data has been permanently erased from the HDD by checking that the “ERASING DATA” message on the LCD display, if displayed on the control panel, has disappeared properly.

- **OE.HDD_ERASE**
  e-STUDIO administrators must ask service engineers to execute the forcible Data Overwrite function on the HDD to permanently erase all user document data.

5. IT SECURITY REQUIREMENTS

This chapter describes the security requirements for the TOE and the IT environment.

5.1 TOE Security Requirements

5.1.1 TOE Security Functional Requirements

The following are the security functional requirements for the TOE.

- 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 [selection: *allocation of the resource to,* ***deallocation of the resource from***] the following objects: [assignment: *list of objects*].

  [assignment: *list of objects*]
  The areas in the HDD of the e-STUDIO352/452 from which user document data was deleted by the operation system's file delete function

  Dependencies: No dependencies.

- FDP_RIP.2 Full residual information protection
  Hierarchical to: FDP_RIP.1
  FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to,* ***deallocation of the resource from***] all objects.

  Dependencies: No dependencies.

- FPT_RVM.1 Non-bypassability of the TSP
  Hierarchical to: No other components.
  FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

  Dependencies: No dependencies.

5.1.2 TOE Security Assurance Requirement

The target assurance level for the TOE is EAL3. The security assurance components of the TOE are as described below:

- ACM_CAP.3 Authorization controls
- ACM_SCP.1 TOE CM coverage
- ADO_DEL.1 Delivery procedures
- ADO_IGS.1 Installation, generation, and start-up procedures
- ADV_FSP.1 Informal functional specification
- ADV_HLD.2 Security enforcing high-level design
- ADV_RCR.1 Informal correspondence demonstration
- AGD_ADM.1 Administrator guidance
- AGD_USR.1 User guidance
- ALC_DVS.1 Identification of security measures
- ATE_COV.2 Analysis of coverage
- ATE_DPT.1 Testing: high-level design
- ATE_FUN.1 Functional testing
- ATE_IND.2 Independent testing - sample
- AVA_MSU.1 Examination of guidance
- AVA_SOF.1 Strength of TOE security function evaluation
- AVA_VLA.1 Developer vulnerability analysis

5.1.3 Minimum Strength of Function Declaration

The minimum Strength of Function (SOF) claim for the TOE is SOF-basic.
There are no probabilistic or permutational mechanisms in the TOE that the SOF claims.

5.2 Security requirements for the IT environment

There are no security functional requirements for the IT environment.

6. TOE SUMMARY SPECIFICATION

This chapter describes the TOE summary specification.

6.1 TOE Security Functions

As Table 6.1-1 below shows, the TOE security functions described in Section 6.1.1 satisfy the security functional requirements described in Section 5.1.1.

	FDP_RIP.1	FDP_RIP.2	FPT_RVM.1
SF.TEMPDATA_OVERWRITE	✓		✓
SF.STOREDATA_OVERWRITE		✓	✓

Table 6.1-1 Correspondences between TOE Security Functions and Security Functional Requirements

6.1.1 TOE Security Functions

The following describes the TOE security functions.

SF.TEMPDATA_OVERWRITE
The TOE must provide the following protection for user document data deleted from the HDD of the STUDIO352/452, erase the user document data registered with the trash box, and prevent the deleted user document data from being recovered or decoded.

[Residual Information Protection]

- In normal mode, this protection registers it with the trash box where user document data, deleted from the HDD of the e-STUDIO352/452, is to be stored.
- In addition, the protection permanently overwrites it which was registered with the trash box where the user document data, deleted from the HDD of the e-STUDIO352/452, are stored. The method used here is DoD5220.22-M of the US Department of Defense.

(FDP_RIP.1)

Also, in order to prevent this function from being bypassed, the TOE must always execute SF.TEMPDATA_OVERWRITE whenever user document data is used by the e-STUDIO General Functions, by permanently erasing the allocated areas in the trash box where the user document data, deleted from the HDD of the e-STUDIO352/452, are stored and by deallocating such storage areas.
(FPT_RVM.1)

SF.STOREDATA_OVERWRITE
The TOE must provide the following protection for all user document data to be collectively deleted from the HDD of the e-STUDIO352/452, deallocate the storage areas in the trash box, and prevent the deleted user document data from being recovered or decoded.

[Residual Information Protection]

- In self-diagnostic mode, this protection collectively and permanently overwrites all areas of the HDD. The method used here is DoD5220.22-M of the US Department of Defense.

(FDP_RIP.2)

Also, in order to prevent this function from being bypassed, the TOE must execute SF.STOREDATA_OVERWRITE from the operation panel to overwrite all areas of the HDD and deallocate such areas.
(FPT_RVM.1)

6.1.2 Security Mechanism

The table below shows the security mechanism referred to in this ST and used by the TOE security functions.

Security Mechanism	Security Functions
DoD5220.22-M	SF.TEMPDATA_OVERWRITE
	SF.STOREDATA_OVERWRITE

Table 6.1 Security Mechanism and TOE Security Functions

DoD5220.22-M-compliant: 0x00 Fill + 0xFF Fill + random number Fill + validation

6.1.3 Strength of Function Statement

The TOE contains no security functions that are realized by a non-cryptographic and probabilistic or permutational mechanisms.

6.2 Assurance Measures

The documents provided as security assurance measures of the TOE which satisfy the security assurance requirements are as described below:

Assurance Class	Assurance Components	Documents and TOE
ACM Configuration management	ACM_CAP.3 ACM_SCP.1	Configuration List of System Software for e-STUDIO352/452* Configuration Management Plan for System Software for e-STUDIO352/452*
ADV Development	ADV_FSP.1 ADV_HLD.2	Functional specification*/High-level design*
	ADV_RCR.1	Representation correspondence*
ALC Lyfe cycle definition	ALC_DVS.1	Development security*
ATE Tests	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2	Functional tests* TOE
AVA Vulnerability assessment	AVA_MSU.1	Operator's Manual [Common]* Operator's Manual for Basic Function (North America) Operator's Manual for Basic Function (Europe) Data Overwrite Kit
	AVA_VLA.1 AVA_SOF.1	Vulnerability analysis*
AGD Guidance documents	AGD_ADM.1 AGD_USR.1	Operator's Manual [Common]* Operator's Manual for Basic Function (North America) Operator's Manual for Basic Function (Europe) Data Overwrite Kit Insertion Sheet**
ADO Delivery and operation	ADO_IGS.1	SERVICE MANUAL [Overview]* SERVICE MANUAL [Service]* SERVICE MANUAL SERVICE HANDBOOK GP-1060 for e-STUDIO352/452
	ADO_DEL.1	Delivery procedures of the e-STUDIO series' TOE* Delivery procedures of the System Software*

Table 6.2-1 Security Assurance Measures and Security Assurance Requirements

Note: An asterisk (*) in the table above indicates the document is available only in Japanese.
Two asterisks (**) in the table above indicate the document is available both in Japanese and English.

7. PROTECTION PROFILE (PP) CLAIMS

The TOE does not claim conformance to a PP.

8. RATIONALE

This chapter describes the rationale for the security objectives, security requirements, TOE summary specification, and PP claims.

8.1 Security Objectives Rationale

8.1.1 Necessity of Security Objectives

The table below shows the mapping of security objectives to assumptions and threats and demonstrates that each security objective for the TOE is effective for at least one of the assumptions and threats.

	T.TEMPDATA_ACCESS	T.STOREDATA_ACCESS
O.TEMPDATA_OVERWRITE	✓	
OE.OVERWRITE_COMPLETE	✓	
O.STOREDATA_OVERWRITE		✓
OE.HDD_ERASE		✓

Table 8.1-1 Security Objectives to Assumptions and Threats

8.1.2 Sufficiency of Security Objectives

This section describes sufficiency of security objectives against the TOE security environment (assumptions and threats).

- **T.TEMPDATA_ACCESS**
  O.TEMPDATA_OVERWRITE can prevent user document data, deleted from the HDD of the e-STUDIO352/452, from being recovered and decoded.
  OE.OVERWRITE_COMPLETE ensures that O.TEMPDATA_OVERWRITE was successfully performed.
  Accordingly, an attack method to **T.TEMPDATA_ACCESS** is invalidated.

- **T.STOREDATA_ACCESS**
  OE.HDD_ERASE allows e-STUDIO administrators to ask service engineers to execute Data Overwrite function on the HDD to permanently erase all files from the HDD.
  O.STOREDATA_OVERWRITE can prevent user document data, all files of which were permanently erased from the HDD of the e-STUDIO352/452 by the forcible Data Overwrite function, from being recovered and decoded.
  Accordingly, an attack method to **T.STOREDATA_ACCESS** is invalidated.

8.2 Security Requirements Rationale

8.2.1 Necessity of Security Functional Requirements

The table below shows relations between security functional requirements and security objectives and demonstrates that each security functional requirement corresponds to at least one security objective.

	O.TEMPDATA_OVERWRITE	O.STOREDATA_OVERWRITE
FDP_RIP.1	✓	
FDP_RIP.2		✓
FPT_RVM.1	✓	✓

Table 8.2-1 Correspondences between TOE Security Functional Requirements and TOE Security Objectives

8.2.2 Sufficiency of Security Functional Requirements

This section describes that the functional requirements sufficiently assure the security objectives for the TOE.

- **O.TEMPDATA_OVERWRITE**
  FDP_RIP.1 ensures permanent deletion.
  FPT_RVM.1 reliably prevents the security functions from being bypassed.
  Accordingly, the security objective can be realized, which prevents storage areas for user document data, deleted from the HDD of the e-STUDIO352/452, from being recovered and decoded.

- **O.STOREDATA_OVERWRITE**
  FDP_RIP.2 ensures collective, permanent, and forcible deletion.
  FPT_RVM.1 reliably prevents the security functions from being bypassed.
  Accordingly, the security objective can be realized, which prevents storage areas for user document data, all files of which were deleted from the HDD of the e-STUDIO352/452, from being recovered and decoded.

8.2.3 Rational for Dependencies of Security Functional Requirements

This section describes the rationale for the dependencies of the security functional requirements.

- **FDP_RIP.1**
  There are no dependencies to be satisfied.

- **FDP_RIP.2**
  There are no dependencies to be satisfied.

- **FPT_RVM.1**
  There are no dependencies to be satisfied.

8.2.4 Mutually Supportive Security Requirements

This section describes that the security functional requirements, mutually complement with each other, are protected against bypass, interference, and deactivation.

Note that FDP_RIP.1 and FDP_RIP.2 do not function simultaneously because each of them functions in different mode.

- **FPT_RVM.1** <Non-bypassability>
  FPT_RVM.1 ensures that FDP_RIP.1 in normal mode or FDP_RIP.2 in self-diagnostic mode functions without being bypassed.

- <No interference>
  It is impossible to externally modify the TOE itself because it resides in the ROM to control overall e-STUDIO352/452. And, there are no unauthorized subjects which modify the TSF data (information in the trash box). Therefore, there are preventive measures against interference by unreliable subject and no

functional requirements are required to prevent the security functions from being modified.

- <Prevention of Deactivation>
  There are no functions which deactivate the security functions of the TOE.

8.2.5 Validity of Minimum Strength of Function

As it is assumed that attackers' attack capabilities is low, the appropriate minimum SOF is SOF-basic.

8.2.6 Rationale for Security Assurance Requirements

The TOE is used in general office environments. Therefore, regarding the TOE, opportunities of attack are limited and low attack capabilities of threat agents can be assumed.

In order to cope with the attacks by the threat agents, security measures, which must be analyzed during the development of the TOE (systematic analysis and test of design, and security assurance of development environment), are to be evaluated. Therefore, an appropriate assurance level for the TOE is EAL3.

8.3 TOE summary specification rationale

8.3.1 Necessity of Security Functions

The table below shows relations between TOE security functions and security functional requirements and demonstrates that each TOE security function corresponds to at least one TOE security functional requirement.

	FDP_RIP.1	FDP_RIP.2	FPT_RVM.1
SF.TEMPDATA_OVERWRITE	✓		✓
SF.STOREDATA_OVERWRITE		✓	✓

Table 8.3-1 Correspondences between TOE Security Functions and Security Functional Requirements

8.3.2 Sufficiency of Security Functions

This section describes that the security functions fully assure the security functional requirements for the TOE.

- **FDP_RIP.1**
  SF.TEMPDATA_OVERWRITE permanently erases user document data in the HDD of the-STUDIO352/452 to ensure that user document data, deleted from the HDD, are no longer available.
  Accordingly, residual information protection is assured by **SF.TEMPDATA_OVERWRITE.**

- **FDP_RIP.2**
  SF.STOREDATA_OVERWRITE collectively and permanently erases all areas of the HDD of the e-STUDIO352/452 including user document data stored there to ensure that all user document data in the HDD are no longer available.
  Accordingly, residual information protection is assured by **SF.STOREDATA_OVERWRITE.**

- **FPT_RVM.1**
  SF.TEMPDATA_OVERWRITE permanently erases user document data whenever they are deleted from the HDD of the e-STUDIO352/452.
  In addition, **SF.STOREDATA_OVERWRITE** collectively and permanently erases all user document data whenever they are deleted from the HDD of the e-STUDIO352/452.
  Accordingly, no-bypassability is assured by **SF.TEMPDATA_OVERWRITE** and **SF.STOREDATA_OVERWRITE**.

8.3.3 Rationale for Strength Of Function

There are no security functions which have probabilistic or permutational mechanisms for which rationale must be

provided.

8.3.4 Rationale for Assurance Measures

This section describes the rationales which demonstrate that security measures for the TOE satisfy the assurance requirements. Each security assurance requirement to meet EAL3 corresponds documents and TOE which are security assurance measures.
Such documents and TOE can provide all evidences for the security assurance requirements.
Table 8.3-2 below shows the details of each assurance measure.

Assurance Class	Assurance Components	Documents and TOE	Descriptions
ACM Configuration management	ACM_CAP.3 ACM_SCP.1	・Configuration List of System Software for e-STUDIO352/452* ・Configuration Management Plan for System Software for e-STUDIO352/452*	These documents describe the configuration management method for the TOE. Also they describe references and configuration list for the TOE, CM plan, and CM system.
ADV Development	ADV_FSP.1 ADV_HLD.2	Functional specification*/ High-level design*	These documents describe the TOE security functions (TSF) from the viewpoint of the behavior of the TSF and TSF interface, external interfaces for functions other than the TSF (functional specifications) and the sub-system. In addition, they describe the TSF structure and interface of the sub-system (High-level design).
	ADV_RCR.1	Representation correspondence*	This document provides analysis report on relations between security functions in the summary specification and the subsystem in the functional specification/high-level design for the ST.
ALC Life Cycle Definition	ALC_DVS.1	Development security*	This document describes the means for assuring confidentiality and integrity of the design and implementation of the TOE in the development environment.
ATE Tests	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2	・Functional tests* ・TOE	These document describe functional test items and test procedures used for proving that the TSF functions are as specified, expected test results, and actual test results under the above-mentioned conditions.

Assurance Class	Assurance Components	Documents and TOE	Descriptions
AVA Vulnerability assessment	AVA_MSU.1	・Operator's Manual [Common]* ・Operator's Manual for Basic Function (North America) ・Operator's Manual for Basic Function (Europe) ・Data Overwrite Kit	These documents describe the procedures to help the TOE users securely install the product and software and perform operations.
	AVA_VLA.1	Vulnerability analysis*	This document describes the result of vulnerability analysis to ensure that obvious security vulnerability found will not be wrongfully used in TOE environments.
	AVA_SOF.1		This document describes the analysis result of strength of function for security mechanisms which have probabilistic or permutational mechanisms excluding cryptographic mechanism for the TOE.
AGD Guidance documents	AGD_ADM.1 AGD_USR.1	・Operator's Manual [Common]* ・Operator's Manual for Basic Function (North America) ・Operator's Manual for Basic Function (Europe) ・Data Overwrite Kit ・Insertion Sheet**	These documents describe the procedures to help the TOE users securely install the product and software and perform operations.
ADO Delivery and operation	ADO_IGS.1	・SERVICE MANUAL [Overview]* ・SERVICE MANUAL [Service]* ・SERVICE MANUAL ・SERVICE HANDBOOK GP-1060 for e-STUDIO352/452	
	ADO_DEL.1	・Delivery procedures of the e-STUDIO series' TOE* ・Delivery procedures of the System Software*	

Table 8.3-2 List of Security Assurance Measures

Note: An asterisk (*) in the table above indicates the document is available only in Japanese.
Two asterisks (**) in the table above indicate the document is available both in Japanese and English.

8.4 PP Claim rationale

There are no Protection Profiles (PPs) to which this ST is conformant.