TOSHIBA

e-STUDIO520/600/720/850
e-STUDIO523/603/723/853

System Software

Security Target

22 July 2008
Ver 3.3

This document is a translation of the evaluated and certified security target written in Japanese.

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	:	e-STUDIO520/600/720/850, e-STUDIO523/603/723/853 System Software Security Target
ST Version	:	Ver3.3
Publication Date	:	22 July 2008
Authors of ST	:	Document Processing & Telecommunication Systems Company, TOSHIBA TEC CORPORATION
TOE Identification		
[Japanese]	:	e-STUDIO520/600/720/850, e-STUDIO523/603/723/853 System Software
[English]	:	System Software for e-STUDIO520/600/720/850, e-STUDIO523/603/723/853
TOE Version	:	V2.0
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 2.3 CCIMB Interpretations (as of August 2005)
Evaluation Methodology	:	Common Methodology for Information Technology Security Evaluation Version 2.3 CCIMB Interpretations (as of August 2005)

1.2 ST Overview

The TOE which this ST defines is the control software for the TOSHIBA TEC CORPORATION's MFP, "the e-STUDIO520/600/720/850 and the e-STUDIO523/603/723/853." The TOE is enabled when the security functions of the e-STUDIO are activated by the optional product GP-1060.
The MFP is a digital multi function device which inputs and processes user documents. Its main functions include copying, printing, faxing, and the e-Filing Box/shared folder feature.
When these functions are used, user document data input into the MFP is temporarily written into the HDD and deleted after the processing is finished. However, the deletion in the FAT file system does not erase the data permanently, leaving them recoverable. This is also the case with the deletion of the user document data saved in the e-Filing Box/shared folder.

The TOE ensures that the deletion of the user document data written into the HDD while using the MFP functions erases them permanently from the HDD in an unrecoverable manner. In addition, before the HDD is disposed of or replaced, a service engineer erases the data in the all memory areas of the e-Filing Box/shared folder, permanently erasing all the document data in the HDD.

1.3 CC Conformance

This ST conforms to the following CC specifications:

- CC Version 2.3, Part 2 conformant
- CC Version 2.3, 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 mainly copying, scanning, printing, and faxing.

- e-STUDIO
  MFPs. In this ST, it refers to the e-STUDIO520/600/720/850 and the e-STUDIO523/603/723/853 (e-STUDIO520, e-STUDIO600, e-STUDIO720, e-STUDIO850, e-STUDIO523, e-STUDIO603, e-STUDIO723, and e-STUDIO853).

- e-STUDIO General Functions
  Copying, scanning, printing, faxing, and the e-Filing Box/shared folder functions that are installed into the e-STUDIO and available for general users.

- Job
  A unit used for the processing of the General Functions. The user document data temporarily written into the HDD for the processing during a job or when a job is finished (or cancelled) are permanently erased by the TSF.

- User document
  Documents that users possess, such as Word, Excel, PDF, and text documents and JPEG images.

- User document data
  Computerized user documents which exist in the MFP. This includes user documents computerized and input by the scanner, computerized documents that the MFP has received, and the data generated by processing them in the MFP.

- Deletion
  To release the resources and make data unavailable for users.

- Erasing
  To erase data without leaving traces.

- Perfect erasing
  To permanently erase data to prevent the reuse of user document data by overwriting the areas for the data to be deleted with meaningless data.

- TopAccess
  A web-based job/device management tool which enables users to obtain information about MFP via the Internet and use two types of web sites, for users and for administrators.

- e-Filing Box
  The location where users save user document data. After saving data, users can refer to, print, or edit them with the control panel or the TopAccess. When the file saving period expires, the saved user document data are deleted. There are two types of e-Filing Boxes: public boxes, which have no access limitations, and user

boxes, which users can create after setting a password.

- Shared folder
  The location where users can save user document date in file formats such as JPEG and PDF and obtain files from client PCs on the Internet. When the file saving period expires, the saved user document data are deleted.

- Internet fax
  Communicates through LAN network using Emails to send original documents in TIFF-FX (Profile S) - format attached files. One of its advantages is less communications cost and higher resolution than normal facsimile. Data can be sent and received via the Internet fax between compatible models. In addition, documents and images can be sent from a PC and received by a compatible model as the Internet fax. When they are sent from a compatible model to a PC, they are received as Emails by the PC. When the main unit receives the Internet fax, it automatically output it just as normal facsimile.

- WS scanning
  WS (Web Service) scanning is a function that performs scanning operations with Windows Vista computers via networks using functions of the computer. Images scanned by the main unit can be saved into a computer. In addition, images can be acquired by sending a scanning request from a WIA (Windows Imaging Acquisition) Scan Driver-compatible application to the main unit.

- GP-1060
  A product installed in the e-STUDIO to enable the Data Erasing Function, a security function of the System Software

1.5 Trademark Notice

- VxWorks is a registered trademark or trademark of Wind River Systems, Inc.
- The formal name of Windows Vista is Microsoft Windows Vista Operating System.
- Microsoft, Windows, Windows NT, and the names and the product names of other Microsoft products are registered trademarks or trademarks in USA or other countries of Microsoft Corporation, USA.
- Firefox and Thunderbird are registered trademarks or trademarks in USA or other countries of Mozilla Foundation, USA.
- 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-STUDIO520/600/720/850 and the e-STUDIO523/603/723/853.

2.1 Product Type and Usage Environment

This ST defines eight types of MFPs, the e-STUDIO520, e-STUDIO600, e-STUDIO720, e-STUDIO850, e-STUDIO523, e-STUDIO603, e-STUDIO723, and e-STUDIO853, each having different print speed. The TOE is the common control software among them.
As shown in Figure 2.1 below, the e-STUDIO is 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 it is installed in general offices as a standalone copier.

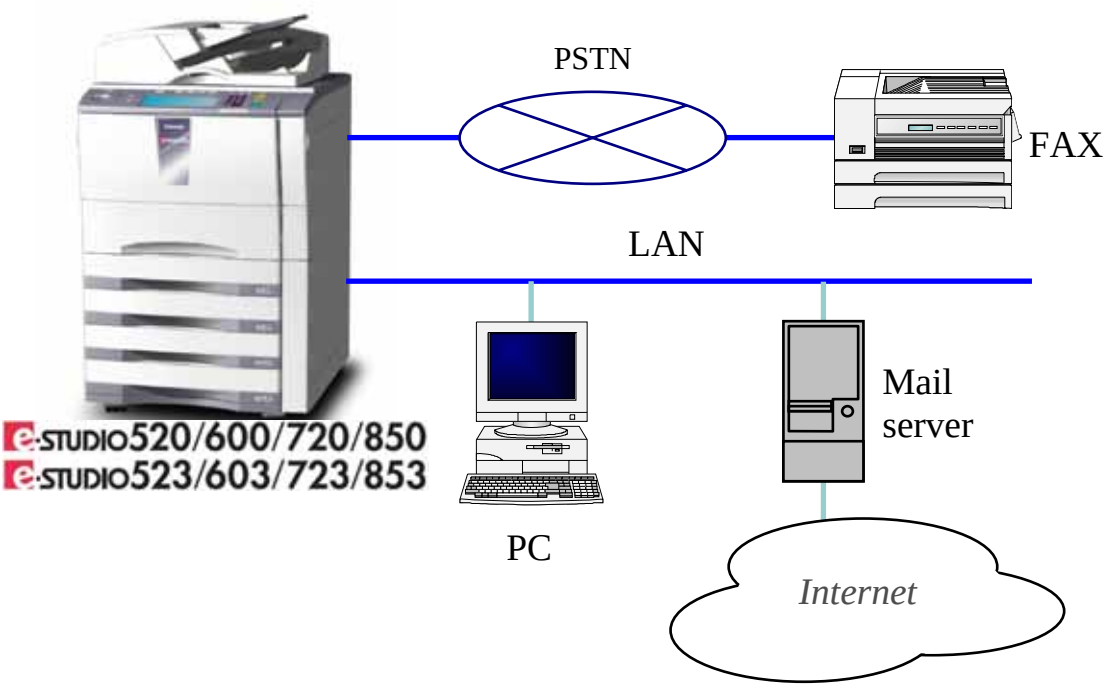

Figure 2.1 Use of the e-STUDIO in Network Environment

The security functions, optional functions of the e-STUDIO can be enabled when a service engineer connects the security enabler GP-1060 to the e-STUDIO. The security functions of the TOE are always enabled.
The enabled security functions erase user document data in an unrecoverable manner when the user deletes them during a job specified by the user or after the job is finished (or cancelled).

Using e-STUDIO General Functions temporarily stores the user document data from the scanner or the LAN/FAX/USB lines into the HDD of the MFP. Then, printing, faxing, or saving into the e-Filing Box/shared holder is performed using the data. The user document data temporarily stored in the process will be deleted as soon as they become unnecessary.
If the security functions are not enabled then, the file is deleted by the file delete function provided by OS. In this case, only the file area pointer of the FAT32 (File Allocation Table) managed by OS is cleared, and the area with the user document data that the e-STUDIO user never imagines exist in the HDD still remains in the e-STUDIO. Furthermore, past data exist as remnant magnetism even after they are overwritten with new data. Therefore, an attacker with knowledge of OS and data recovering tools can remove the HDD and then read the reference of the actual data, which have lost only the pointer, and the remnant magnetism of the data and retrieve information, posing a huge threat. Similarly, when the data in the e-Filing Box/shared folder are deleted, a fear exists that the data that the user believes are deleted can be read.

The data erasing function, a security function in normal mode of the TOE (2.2.1.2 Security Functions in Normal Mode) permanently erases the deleted user document data. As long as the security function is enabled, erasing residual data does not require special operations by users.

In addition, overwrite erasing compulsion execution processing of the security functions in self-diagnostic mode (2.2.2.2 Security Functions in Self-Diagnostic Mode) collectively and permanently erase the user document data left saved in the e-Filing Box/shared folder when the HDD is disposed of or replaced. As this function works in self-diagnostic mode, it is enabled by a service engineer.

Hardware Configuration	Specification
e-STUDIO520/600/720/850 e-STUDIO523/603/723/853	e-STUDIO520/523: 52 sheets/min. e-STUDIO600/603: 60 sheets/min. e-STUDIO720/723: 72 sheets/min. e-STUDIO850/853: 85 sheets/min. Copy/print speed on A4-size or LETTER-size papers
GP-1060	USB interface

Table 2.1-1 e-STUDIO Hardware Configuration

Software Configuration	Function
System Software V2.0	System Software for controlling the e-STUDIO520/600/720/850 and the e-STUDIO523/603/723/853
UI data (Optional languages) Japanese: V055.000 2 American English: V062.000 3 European English: V058.000 4	Language data for each destination (nation)
VxWorks 5.5	OS

Table 2.1-2 e-STUDIO Software Configuration

Software such as Printer Driver, Fax Driver, Web Browser, or Mailer is required in PC, to use in normal mode of 2.2.1 in Figure 2.1 configuration.

- Printer Driver
  e-STUDIO850 Series PrinterDriver Ver 4.4.63.0
- Fax Driver
  e-STUDIO850 Series N/W-Fax Driver Ver 4.9.60.0
- Browser
  InternetExplorer ver6.0 sp1 or Firefox ver2.0.0.14
- Mailer
  AL-Mail32 Version1.13 or Thunderbird ver2.0.0.14
- WIA Scan Driver Application
  Windows Fax and Scan Version 6.0

2.2 Product Functions and TOE

This product is a digital multi function device in which e-STUDIO General Functions, that is, copying, scanning, printing, faxing, and the e-Filing Box/shared folder functions are installed.

The TOE is software for the e-STUDIO which resides in its ROM and conducts overall control on it.

The e-STUDIO starts in normal mode, where users operate it.

In normal mode, the e-STUDIO General Functions and the security functions 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 the 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-STUDIO 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.

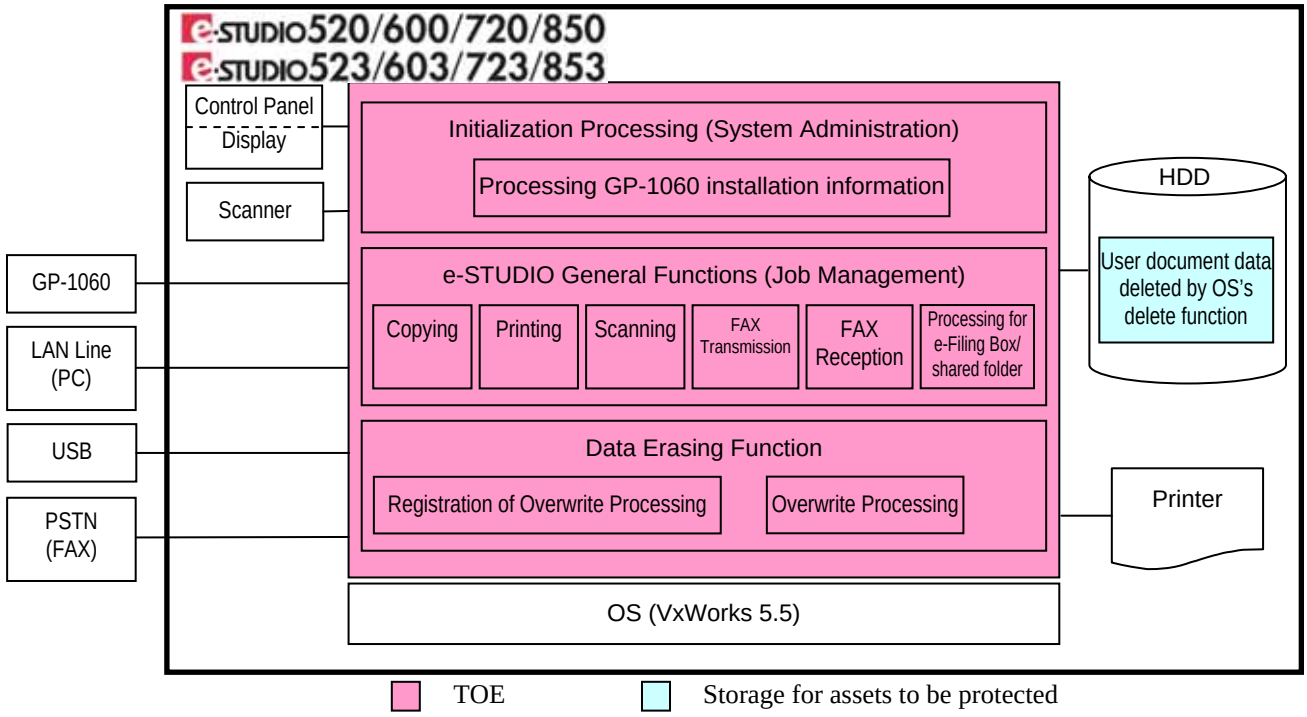

Figure 2.2.1 Product Configuration in Normal Mode

2.2.1.1 e-STUDIO General Functions in Normal Mode

(1) Processing 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 Erasing Function is available, an icon representing data erasing and the TOE version are displayed on the “Setting/Registration” screen of the control panel.

(2) Copying
When the START button is pressed with the copying function selected, this function scans user document data using the scanner and writes the scanned data into the work area of the HDD.
Then, this function reads the user document data in the work area and performs both or either of the following processings:

- 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) Printing
This function receives user document data via a LAN line (PC) or a USB, or reads user document data in an e-Filing Box, and writes the data in the work area of the HDD.
Then, this function reads the user document data in the work area and performs both or either of the following processings:
- 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) Scanning
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 processings:
- Saves the user document data in an e-Filing Box or a shared folder in the HDD specified by the e-STUDIO user or sends the data to computer(s) specified with WS scanning.
- Sends Email to a destination specified by the e-STUDIO user.

(5) Fax transmission
When the START button is pressed while the FAX button is being held down, this function scans user document data using the scanner and writes the scanned data in the work area of the HDD.
Then, this function 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
This function receives user document data from a facsimile and writes the data in the work area of the HDD.
Then, this function reads the user document data in the work area and performs both or either of the following processings:
- 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) Processing for e-Filing Box and shared folder
This function 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 Erasing Function)

There are two security functions in normal mode: Data Overwrite registration processing and Data Overwrite processing. These two functions are altogether called the data erasing function.

(1) Data Overwrite registration processing
The Data Overwrite registration processing is started up when user document data are deleted in the processings of the e-STUDIO General Functions (2) to (7). In this processing, only the path for the user document data with a deletion request is moved to the trash box (renamed). This processing makes the deleted files those for the Data Overwrite processing.

(2) Data Overwrite process
This function checks if user document data has been registered with the trash box and, if any has been registered, permanently erases the storing area. While this processing 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-STUDIO 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.

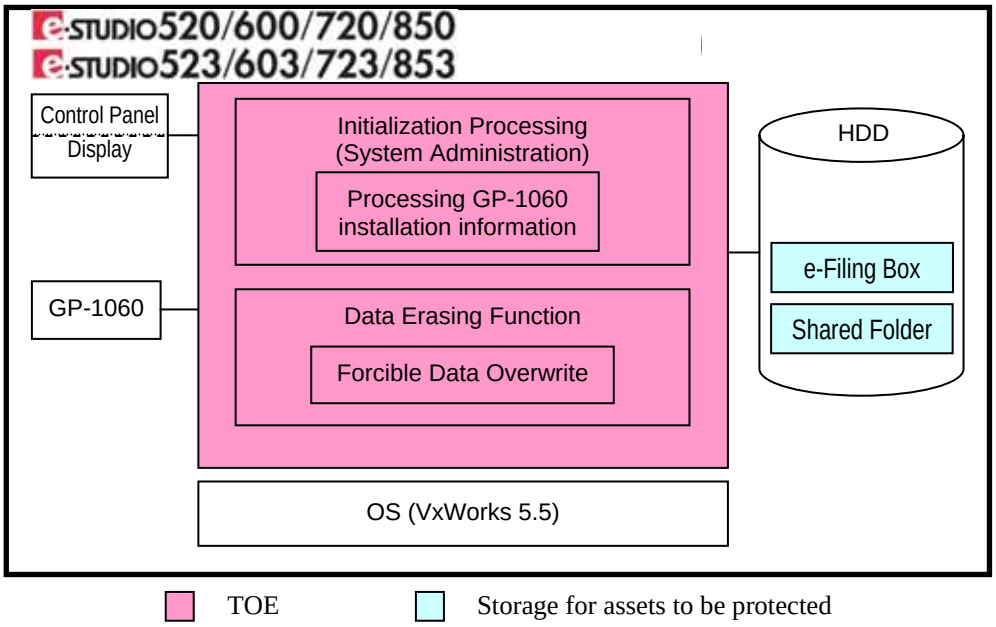

Figure 2.2.2 Product Configuration in Self-diagnostic Mode

2.2.2.1 e-STUDIO General Functions in Self-diagnostic Mode

Although e-STUDIO General Functions in self-diagnostic mode have the settings for maintenance and display the device information, only the security function-related processings shown below are described here.

- Processing GP-1060 Installation Information
  This process checks whether or not the GP-1060 is installed. Although whether the Data Erasing Function is enabled is not displayed on the screen for service engineers, the security functions in self-diagnostic mode described in 2.2.1.4 can be used if they are enabled.

2.2.2.2 Security Functions in Self-diagnostic Mode

- Forcible Data Overwrite processing
  It collectively and permanently erases all areas where user document data which are stored in HDD are written.

2.3 TOE-related Personnel

The following describes personnel required for operating the TOE.

2.3.1 Users

Users who utilize the e-STUDIO General Functions of the e-STUDIO

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-STUDIO (including installation of the GP1060).
Upon request from the e-STUDIO administrator, a 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-STUDIO where user document data are stored.

2.4 Assets to be Protected

The assets to be protected in normal or self-diagnostic mode are described below.

- Assets to be protected in normal mode
  The data remaining magnetically in the HDD after the deletion of user document data are the assets to be protected. The assets to be protected are generated when the e-STUDIO deletes user document data during the job specified by the user or after it is finished (or cancelled).
  Note that the remaining data from the user document data deleted in the following processings are excluded from the protection target:

  [1] Fax reception
  Since it can be assumed that facsimile senders perform facsimile transmission from a site far away from the TOE and have no means to confirm that the transmitted facsimile data have been erased by the security functions, these data are excluded from the protection target.

  [2] Automatic deletion after the file saving period expires in the e-Filing Box/shared folder
  If the saving period (days) is set, user document data are deleted by the TOE when the period expires. Since it can not be assumed that users will confirm the security functions erase the data every time they are automatically deleted, these data are excluded form the protection target.

- Assets to be protected when the HDD is disposed of or replaced
  The user document data remaining in the HDD of the e-STUDIO to be disposed of or to be replaced are the assets to be protected.

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-STUDIO.

- **T.TEMPDATA_ACCESS**
  A malicious e-STUDIO user or non-privileged user may attempt to retrieve user documents by using off-the-shelf tools to recover and decode user document data deleted from the HDD of the e-STUDIO.

- **T.STOREDATA_ACCESS**
  A malicious e-STUDIO user or non-privileged user may attempt to retrieve user documents from the HDD of the e-STUDIO by using off-the-shelf tools.

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-STUDIO, from which user document data were deleted, in order to prevent such areas from being recovered or decoded.

- **O.STOREDATA_OVERWRITE**
  The TOE must be deleted collectively by forcible data overwriting, not to recover or decode user document data from the HDD of the e-STUDIO which is disposed of or replaced.

4.2 Security Objectives for the Environment

The following are the security objective for the environment.

- **OE.OVERWRITE_COMPLETE**
  When collecting printout from 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, when e-STUDIO is disposed of or the HDD is replaced.

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-STUDIO 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 e-STUDIO, 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-STUDIO, 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-STUDIO, are stored.

(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-STUDIO, 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-STUDIO by forcible data overwrite processing, 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. (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 the e-STUDIO520/600/720/850 and the e-STUDIO523/603/723/853* Configuration Management Plan for System Software for the e-STUDIO520/600/720/850 and the e-STUDIO523/603/723/853*
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	Quick Start Guide [Japanese]* Quick Start Guide
	AVA_VLA.1 AVA_SOF.1	Vulnerability analysis*
AGD Guidance documents	AGD_ADM.1 AGD_USR.1	Quick Start Guide [Japanese]* Quick Start Guide
ADO Delivery and operation	ADO_IGS.1	SERVICE MANUAL [Overview]* SERVICE MANUAL [Service]* SERVICE MANUAL SERVICE HANDBOOK GP-1060 for the e-STUDIO520/600/720/850 and the e-STUDIO523/603/723/853
	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.

Note: The model numbers vary depending on the destination (country) because the models that are not described in a guidance will not be delivered to the destination (country). (For example, e-STUDIO520 is not described in the guidance for Japan.)

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-STUDIO, 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, when e-STUDIO is disposed of or the HDD is replaced by protecting user document data of the HDD of e-STUDIO from being decoding or recovered.
  O.STOREDATA_OVERWRITE can prevent user document data, all files of which were permanently erased from the HDD of the e-STUDIO 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 deletes stored areas of user document data where files are deleted permanently.
  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-STUDIO, from being recovered and decoded.

- **O.STOREDATA_OVERWRITE**
  FDP_RIP.2 deletes all user document data (object) permanently.
  FPT_RVM.1 reliably prevents the security functions from being bypassed.
  Accordingly, the security objective can be realized, which prevents areas for user document data from the HDD of the e-STUDIO, 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-STUDIO. 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 STUDIO 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-STUDIO 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-STUDIO.
  In addition, **SF.STOREDATA_OVERWRITE** collectively and permanently erases all user document data whenever they are deleted from the HDD of the e-STUDIO by forcible data overwrite processing.

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 the e-STUDIO520/600/720/850 and the e-STUDIO523/603/723/853* ・Configuration Management Plan for System Software for the e-STUDIO520/600/720/850 and the e-STUDIO523/603/723/853*	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 documents 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	・Quick Start Guide [Japanese]* ・Quick Start Guide	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	・Quick Start Guide [Japanese]* ・Quick Start Guide	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 the e-STUDIO520/600/720/850 and the e-STUDIO523/603/723/853	
	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.

Note: The model numbers vary depending on the destination (country) because the models that are not described in a guidance will not be delivered to the destination (country). (For example, e-STUDIO520 is not described in the guidance for Japan.)

8.4 PP Claim rationale

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