TOSHIBA

Security Target For
e-STUDIO205L/255/305/355/455

June 11, 2009
Ver 1.1

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

TOSHIBA TEC CORPORATION

Table of Contents

Terms and Abbreviations

The terms, abbreviations and trademarks used in this ST are described below:

- Resource terms

User document	Documents that users possess, such as Word, Excel, PDF, along with text documents and JPEG images.
User document data	Electronic user documents which exist in the MFP. This includes user documents computerized and input by the scanner, electronic documents that the MFP has received, and the data generated by processing them in the MFP.
Resource	Physical components taking in the TOE, digital components such as built-in fonts and consumables for the TOE such as toner.

• TOE-related terms and abbreviations

MFP (Multifunction Peripherals)	Multifunction peripheral (digital multifunction device), which integrates mainly copy, scan, print and Fax functions into a single device.
e-STUDIO	Multifunction peripheral (digital multifunction device), which integrates mainly copy, scan, print and Fax functions into a single device. In this ST, it refers to the e-STUDIO205L/255/305/355/455.
General functions of the e-STUDIO	Copy, scan, print, Fax and e-Filing Box/shared folder functions, which are integrated into the e-STUDIO and available for general users.
Job	A unit used for processing the general functions of the e-STUDIO. The user document data temporarily written into the HDD for processing during a job or when a job is finished (or cancelled) are permanently erased by the TSF.
TopAccess	A web-based job/device management tool, which enables users to obtain information about the eSTUDIO 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 on the control panel or in TopAccess. When the file retention period expires, the saved user document data are deleted.
Shared folder	The location where users can save user document data in file formats such as JPEG and PDF and obtain files from client PCs on the Internet. When the file retention period expires, the saved user document data are deleted.
Internet Fax	It conducts communications through LAN network to send original documents in TIFF-FX (Profile S) -format attached files by e-mail. One of its advantages is less communications cost and higher resolution than a normal facsimile machine. Data can be sent and received by 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 data are sent from a compatible model to a PC, the PC receives the data as email messages. When receiving an Internet Fax, the main unit automatically outputs it just as a normal facsimile machine does.
WS-Scan	WS (Web Service) Scan is a function that performs scanning on a Windows Vista computer through the network using the 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 scan request from a WIA (Windows Imaging Acquisition) Scan Driver-compatible application to the main unit.
Deletion	To deallocate resources and make data unavailable for users.
Erase	To erase data without leaving traces.
Complete erase	To permanently erase data to prevent the reuse of user document data by overwriting the areas for the data to be deleted with useless data.
GP-1070, GP-1140	Device for security license registration by connecting to the e-STUDIO205L/255/305/355/455. The security functions in the system software are enabled when the license is registered.

• CC-related abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength Of Function
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Function
SFR	Security Functional Requirement

• Trademarks
  - The official 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 the United States and other countries of Microsoft Corporation of the U.S.
  - All other product names mentioned in this ST may be trademarks or registered trademarks of their respective owners.

1. SECURITY TARGET INTRODUCTION

This chapter describes reference to security target (hereinafter referred to as "ST"), reference to target of evaluation (hereinafter referred to as "TOE") and conformance to the Common Criteria (hereinafter referred to as "CC").

1.1 Reference to ST

Information to identify this ST is described below:

ST Title: Security Target for e-STUDIO205L/255/305/355/455
ST Version: Ver1.1
ST Created on: June 11, 2009
ST Created by: Toshiba TEC Corporation
Evaluation Assurance Level: EAL3
Criteria: Common Criteria for Information Technology Security Evaluation
Version 3.1
Part 1: Introduction and general model Revision 1 (CCMB-2006-09-001)
Part 2: Security functional components Revision 2 (CCMB-2007-09-002)
Part 3: Security assurance components Revision 2 (CCMB-2007-09-003)
Evaluation Methodology: Common Methodology for Information Technology Security Evaluation
Version 3.1
Evaluation methodology Revision 2 (CCMB-2007-09-004)

1.2 Reference to TOE

Information to identify this TOE is described below:

TOE Title
[Japanese]: System Software for e-STUDIO205L/255/305/355/455
[English]: System Software for e-STUDIO205L/255/305/355/455
TOE Version: V3.0
TOE Developed by: Toshiba TEC Corporation

1.3 TOE Overview

1.3.1 Explanation about TOE

The TOE defined in this ST is the control software for the MFPs "e-STUDIO205L/255/305/355/455" manufactured by Toshiba TEC Corporation. The TOE is enabled when the security functions of the e-STUDIO are activated by the optional GP-1070 or GP-1140.
The e-STUDIO is a digital multifunction peripheral, which inputs and processes user documents. The main functions include copy, print, Fax and e-Filing Box/shared folder functions.
When these functions are used, user document data input into the e-STUDIO is temporarily written into the HDD and deleted after the processing is finished. However, deletion by the FAT file system does not permanently erase data, leaving them recoverable. This also applies to the deletion of user document data saved in the e-Filing Box/shared folder.

The TOE enables deletion of user document data written into the HDD and permanently erases them from the HDD in an unrecoverable manner when the e-STUDIO functions are used. In addition, before the HDD is disposed of or replaced, a service engineer erases data in all memory areas, permanently erasing all user document data in the HDD.

The e-STUDIO205L and e-STUDIO305 will not be marketed for Japan.

1.3.2 Usage of TOE

This ST defines five types of MFPs, the e-STUDIO205L, e-STUDIO255, e-STUDIO305, e-STUDIO355 and e-STUDIO455, each having a different print speed. The TOE is the common control software among them. As shown in Figure 1.3.2 below, the e-STUDIO is used as a terminal to send/receive data to/from facsimile machines, a terminal to send email messages to email servers, and a remote printer for remote PCs in network environments as well as installed in general offices as a standalone device.

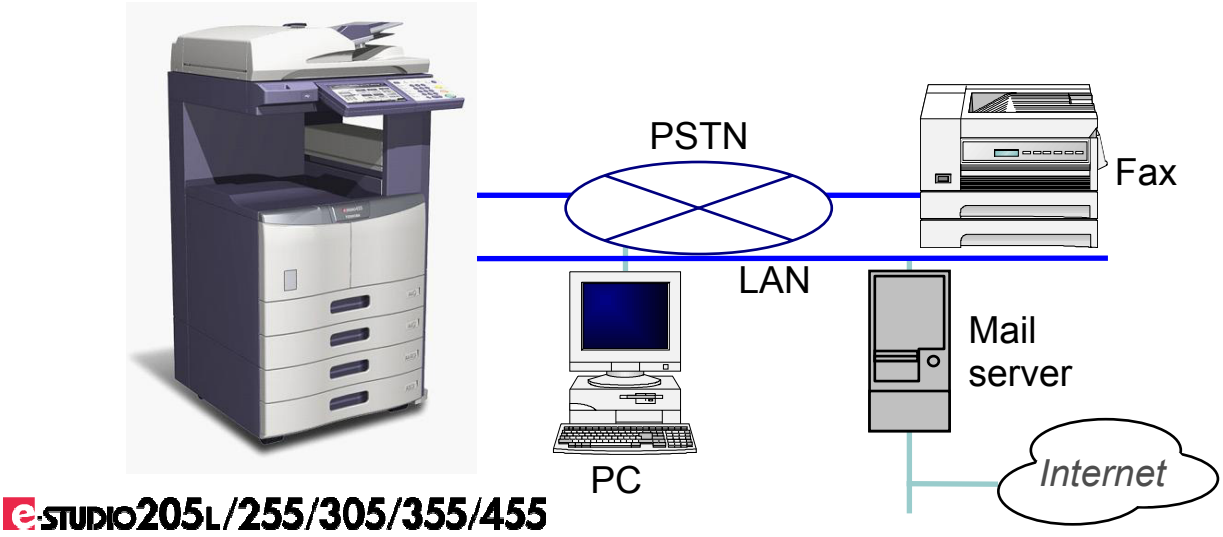


Figure 1.3.2 Use of the e-STUDIO in Network Environment

The security functions as the optional functions of the e-STUDIO are enabled when a service engineer uses the GP-1070 or GP-1140 to register the license in the e-STUDIO. The license of the TOE is always enabled.
The enabled security functions erase data in an unrecoverable manner to delete them in the following situations:
When the e-STUDIO deletes user document data during a job specified by the user or after the job is finished (or cancelled).
When the e-STUDIO automatically deletes expired user document data.

The general functions of the e-STUDIO enable a user to temporarily store user document data from the scanner, LAN, Fax or USB line into the HDD of the e-STUDIO, and then to print, fax or save the data into the e-Filing Box/shared holder. The user document data temporarily stored in the process are deleted by the file delete function provided by OS, as soon as they are no longer needed.
In this case, the file area pointer of the FAT32 (File Allocation Table) managed by OS is only cleared, thus, the area with the user document data recorded, which, the e-STUDIO user may never think, is present in the HDD, still remains in the e-STUDIO. In addition, previous data remain as residual magnetism even after the deleted area is overwritten with new data. Therefore, an attacker with knowledge of OS and data recovery tools may possibly remove the HDD and refer to the actual data with only the pointer reset, or read the residual magnetism of the data and retrieve information, posing a huge threat. Similarly, when the data in the e-Filing Box/shared folder are deleted, the data believed to have been deleted may be read, posing a threat.

The Data Overwrite function as one of the security functions in normal mode of the TOE (1.4.2.2 Security Functions in Normal Mode) permanently erases user document data to be deleted. The user does not need any special operation to erase residual data, as long as the security functions are enabled.
In addition, Forcible Data Overwrite process as one of the security functions in self-diagnostic mode (1.4.2.4 Security Functions in Self-Diagnostic Mode), which collectively and permanently erases remaining data saved in the e-Filing Box/shared folder when the HDD is disposed of or replaced, is provided.

1.3.3 Hardware, software and firmware other than required for TOE

The hardware identified below is required to operate the TOE:

- Identification of hardware and software depended by the security functions of the TOE

Hardware Configuration	Specification (Copy/print speed on A4-size or letter-size paper)
e-STUDIO205L	Monochrome: 20.3 sheets/min.
e-STUDIO255	Monochrome: 25.3 sheets/min.
e-STUDIO305	Monochrome: 30.3 sheets/min.
e-STUDIO355	Monochrome: 35.3 sheets/min.
e-STUDIO455	Monochrome: 45.3 sheets/min.

Software such as printer drivers, Fax drivers, web browsers and mailers is required for the PC to use the functions in normal mode in Figure 1.3.2 Configuration. The following software is installed in the PC to test the TOE:

- Printer driver
  e-STUDIO455 Series Printer Driver Ver 5.15.83.0

- Fax driver
  e-STUDIO Network-Fax Ver 5.15.83.0

- Brower
  Internet Explorer Ver 6.0 SP2

- Mailer
  AL-MaiL32 Version 1.13

- WIA Scan Driver-compliant application
  Windows Fax and Scan Version 6.0

1.3.4 TOE-related Personnel

Personnel and IT equipment for operating the TOE are described below:

- Users
  Users utilize the general functions of the e-STUDIO on the e-STUDIO.

- Administrators
  Administrators configure each setting of the general functions of the TOE (including copy, network and Fax settings) and request service engineers to operate the forcible Data Overwrite function on the HDD.
  Note administrators do not manage the security functions regarding this TOE.

- Service Engineers
  Service engineers perform service maintenance operations such as installation of the e-STUDIO (including security license registration with the GP1070 or GP-1140) in the operation of the e-STUDIO.
  Upon request from the administrator, the service engineer starts the TOE in self-diagnostic mode and operates the forcible Data Overwrite function to collectively and permanently erase all HDD areas, in order to delete user document data in the HDD of the e-STUDIO.

1.3.5 Secured Assets

Secured assets in normal and self-diagnostic modes are described below:

- Secured assets in normal mode
  The remaining magnetic data in the HDD after deletion of user document data indicate secured assets.
  Secured assets are generated in the following situations:
  (1) When the e-STUDIO deletes user document data during a job specified by the user or after the job is finished (or cancelled).
  (2) When the e-STUDIO automatically deletes expired user document data.

- Secured assets when the HDD is disposed of or replaced
  The remaining user document data in the HDD of the e-STUDIO to be disposed of or in the HDD to be replaced indicate secured assets.

1.4 TOE Description

1.4.1 TOE Physical Range

This product is a digital multifunction peripheral, which integrates the general functions of the e-STUDIO, in other words, copy, scan, print, fax and e-Filing Box/shared folder functions.

Among the TOEs, OS is installed on the ROM and any other than OS is installed on the HDD.

When the power to the e-STUDIO is turned on, the e-STUDIO starts in normal mode. Users usually operate the e-STUDIO in this mode.

In normal mode, the general functions of the e-STUDIO (1.4.2.1 General Functions of the e-STUDIO in Normal Mode) and the security functions in normal mode (1.4.2.2 Security Functions in Normal Mode) are available.

In addition to the normal mode, the self-diagnostic mode used for service engineers to perform maintenance services is also provided. When the e-STUDIO starts in self-diagnostic mode, the general functions of the e-STUDIO and the security functions in normal mode are not available.

In this mode, the security functions in self-diagnostic mode (1.4.2.4 Security Functions in Self-Diagnostic Mode) are available.

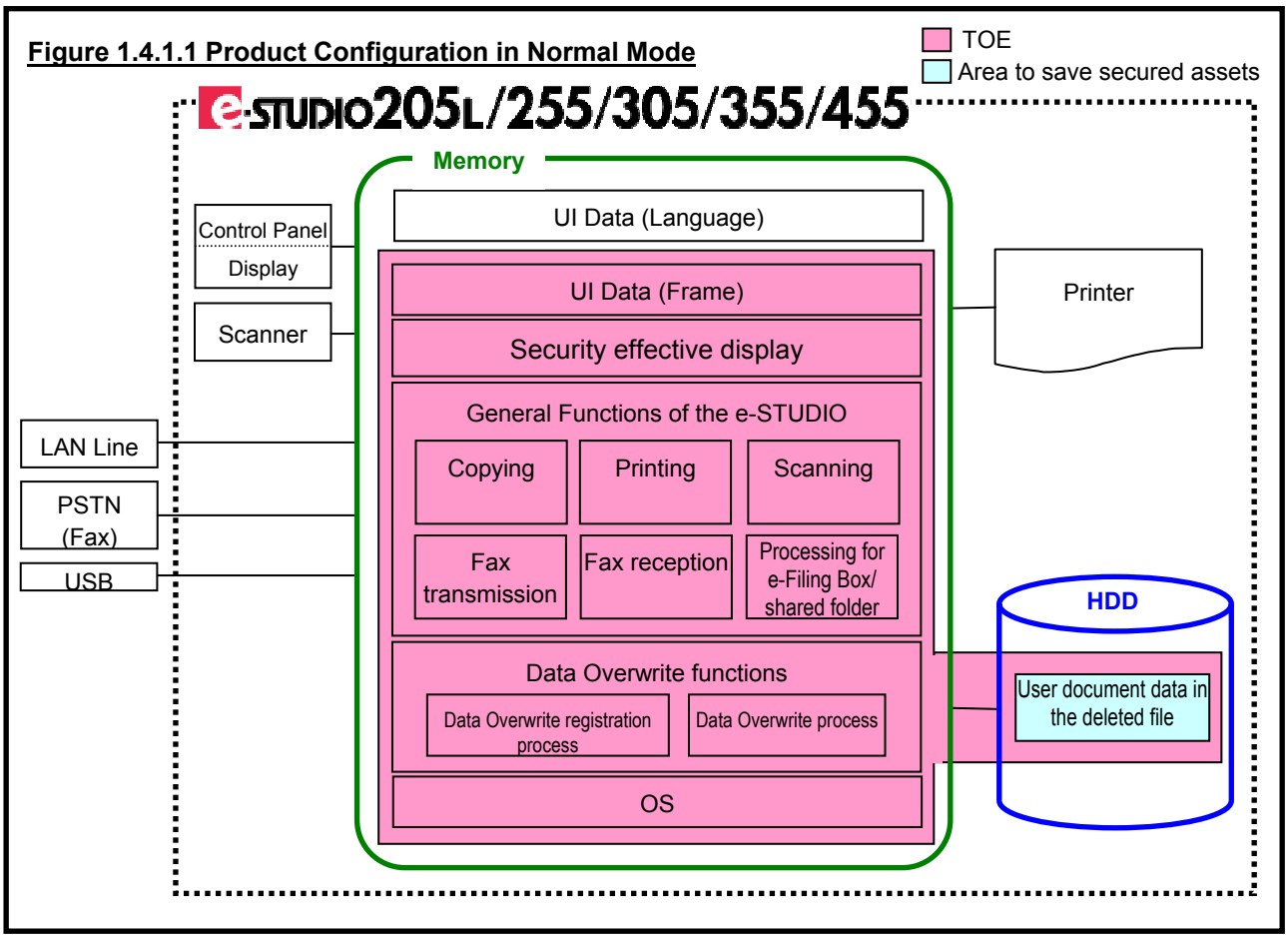
1.4.1.1 Configuration in Normal Mode

The configuration after this product starts in normal mode is shown below:

Figure 1.4.1.1 shows the operable state of this product after the power is turned on and program data is downloaded from the HDD.

User document data exist only in the work area of the HDD, the specified e-Filing Box and shared folder.

The entire system software shown in Figure 1.4.1.1 is the TOE of this ST in normal mode.



Control Panel, Display	Interface composed of the touch panel and operation buttons. Used for copying, printing, scanning, Fax transmission and processing for e-Filing Box/shared folder.
Scanner	Device to read originals.
LAN Line	By connecting to the network, used as a network printer, in TopAccess and for scanning through the network. Used for printing, scanning, Fax transmission and processing for e-Filing Box/shared folder.
PSTN (Fax)	By connecting to the telephone line, used for Fax transmission and reception. Used for Fax reception.
USB	By connecting USB memory storing PDF files, enabling the files to be printed on the control panel, as well as being used as a printer by connecting to a PC with the USB cable. Used for printing and Fax transmission.
Printer	Device for printing.
HDD	Enabling user document data to be saved in the e-Filing Box or shared folder according to the user's operation, as well as storing program data, UI data (language) and setup data. By using the general functions of the e-STUDIO, enabling user document data input into the e-STUDIO to be temporarily written into the HDD. Secured assets in normal mode indicate the remaining magnetic data in the HDD after deletion of user document data.
UI Data (Frame)	Possessing screen configuration information on the panel and TopAccess and controlling the display and screen transition of buttons or messages. Refer to UI data (language) for the displayed buttons or messages.
UI Data (Language)	Storing data corresponding to each language, referred by UI data (frame). Storing buttons or messages in the same configuration each language. Out of the TOE range.

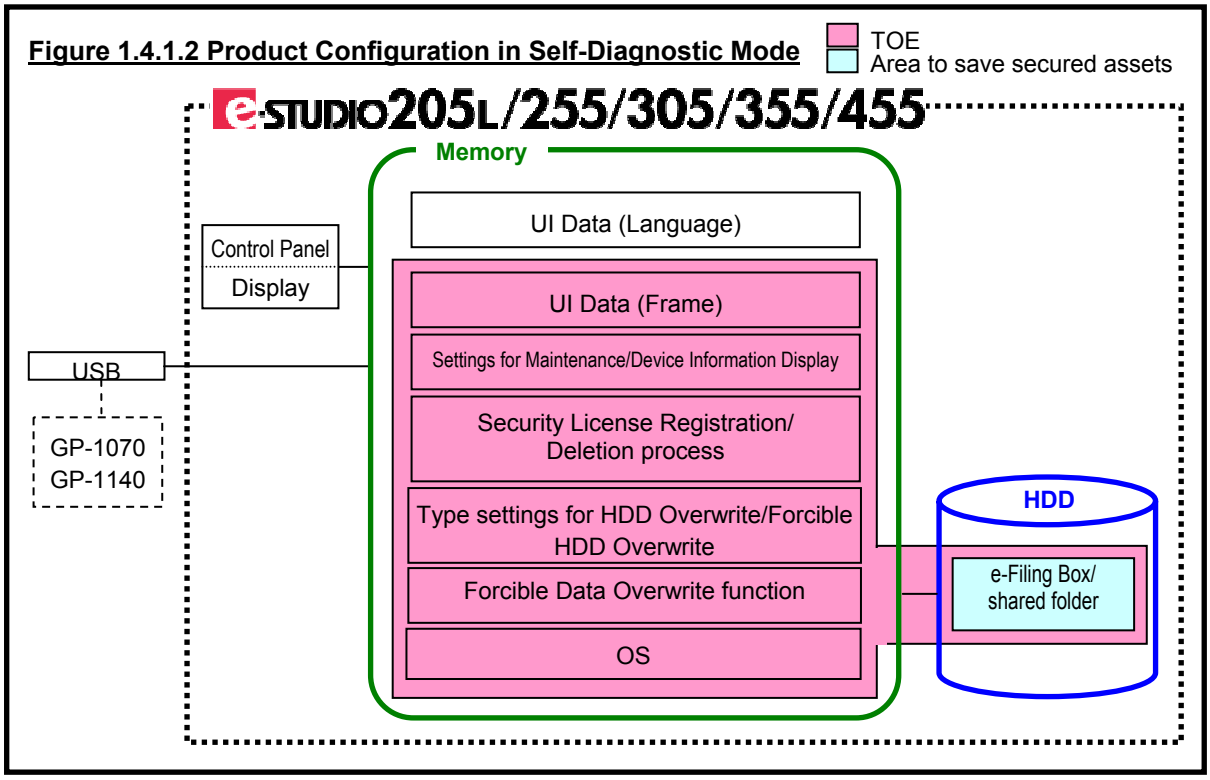
1.4.1.2 Configuration in Self-Diagnostic Mode

The configuration of this product in self-diagnostic mode is shown below:

Figure 1.4.1.2 shows the operable state of this product after the power is turned on and program data is downloaded from the HDD.

The entire system software shown in Figure 1.4.1.2 is the TOE of this ST in self-diagnostic mode.

Figure 1.4.1.2 Product Configuration in Self-Diagnostic Mode



Control Panel, Display	A service engineer starts the self-diagnostic mode on the control panel. In this mode, the forcible Data Overwrite function is enabled when the e-STUDIO is disposed of or the HDD is replaced, as well as maintenance settings. Used for the forcible Data Overwrite function.
USB	Used for connecting the GP-1070 or GP-1140.
GP-1070/GP-1140	Device for security license registration. Operated by a service engineer and to be removed after license registration.
HDD	User document data in the deleted file no longer exist because the general functions of the e-STUDIO are not available in self-diagnostic mode. Secured assets in self-diagnostic mode indicate the remaining user document data in the HDD of the e-STUDIO to be disposed of or in the HDD to be replaced.
UI Data (Frame)	Same as in normal mode. However, TopAccess is not available in self-diagnostic mode.
UI Data (Language)	Same as in normal mode.

1.4.2 Logical Range of TOE

The general functions of the e-STUDIO and security functions are described below:

1.4.2.1 General Functions of the e-STUDIO in Normal Mode

(1) Security effective display

Whether or not the security license is registered is checked.
When the COUNTER button is pressed on the control panel, the print count screen appears. When the security functions are enabled, the icon indicating data overwrite and TOE version [SYS V3.0] are shown.

(2) Copying

When the COPY button is selected on the control panel, the START button is pressed after copy settings, allowing the e-STUDIO to start copying.
The e-STUDIO scans user document data from the scanner, writes them in the work area of the HDD, and outputs the data in the work area from the printer.
In addition, the copy settings enable the data to be saved in the e-Filing Box or shared folder of the HDD, while being output from the printer at the same time. The e-STUDIO saves the data in the work area.

(3) Printing

This function enables the operation to start through LAN and USB lines and on the control panel.

- Start through LAN and USB lines (the eSTUDIO used as a printer)
  The e-STUDIO can be used a network printer on the LAN line or a local printer by connecting to a PC with the USB cable.
  When printing is performed on the connected PC, user document data are sent to the e-STUDIO through LAN lines or USB cables, allowing the e-STUDIO to start printing.
  The settings enable the user document data to be saved in the e-Filing Box.

- Start through LAN lines (TopAccess)
  It is the method of using the e-STUDIO as a printer, enabling the data to be output from the printer through operations in TopAccess or on the panel, instead of directly being output from the printer.
  In TopAccess, when the PRINT menu is open on the JOB tab, a user document desired to print is selected from the list and the RELEASE button is pressed, allowing the e-STUDIO to start printing.

- Start on the control panel
  This function enables a document file in USB media connected to the e-STUDIO to be printed. When the USB button is pressed after selecting the PRINT button on the control panel, the START button is pressed after selecting a document desired to print, allowing the e-STUDIO to start printing.
  As described in Start through LAN lines (TopAccess), the print jobs that are not output from the printer can be output from the printer through operations on the control panel or in TopAccess by allowing the e-STUDIO to start printing. When one of the PRIVATE, HOLD, PROOF and INVALID buttons is pressed after selecting the PRINT button on the control panel, the START button is pressed after selecting a document desired to print, allowing the e-STUDIO to start printing.
  When these interfaces allow the e-STUDIO to start printing, the e-STUDIO writes user document data in the work area of the HDD. The e-STUDIO outputs the data in the work area from the printer. The e-STUDIO saves the user document data in the work area in the e-Filing Box.

(4) Scanning

This function enables the operation to start on the control panel and through LAN lines.

When the SCAN button is selected on the control panel, the START button is pressed after scan settings, allowing the e-STUDIO to start scanning. The e-STUDIO scans user document data from the scanner and writes them in the work area of the HDD. The e-STUDIO saves the data in the work area in the e-Filing Box, shared folder or USB media, or sends them to the specified destination by e-mail.

Start through LAN lines provides a WS Scan function allowing the e-STUDIO on the LAN to be used as a scanner on a Windows Vista PC. The PC sends a scan request to the e-STUDIO, allowing the e-STUDIO to start scanning. The e-STUDIO scans user document data from the scanner and sends image data to the PC that sent a scan request.

(5) Fax transmission

This function enables the operation to start on the control panel and through LAN and USB lines.

- Start on the control panel

  When the FAX button is selected on the control panel, the START button is pressed after Fax settings, allowing the e-STUDIO to start Faxing.

  The e-STUDIO scans user document data from the scanner, writes them in the work area of the HDD, and sends the data in the work area by Fax through PSTN (Fax) or by Internet Fax through LAN lines.

- Start through LAN and USB lines

  The e-STUDIO can be used a network printer on the LAN line or a local printer by connecting to a PC with the USB cable.

  The print settings enable user document data to be sent by Fax or Internet Fax when the Network Fax driver is selected.

  When receiving the user document data from the Network Fax driver, the e-STUDIO starts Fax transmission. The e-STUDIO writes the received user document data in the work area of the HDD, and sends the data in the work area by Fax through PSTN (Fax) or by Internet Fax through LAN lines.

(6) Fax reception

When receiving Fax data through PSTN (Fax) or Internet Fax data through LAN lines, the e-STUDIO starts Fax reception.

The e-STUDIO writes the received user document data in the work area of the HDD, and outputs the data from the printer.

When data are to be saved, the e-STUDIO saves the received data in the specified e-Filing Box or shared folder.

(7) Processing for e-Filing Box/shared folder
When using user document data saved in the e-Filing Box and shared folder, the e-STUDIO starts processing for e-Filing Box and shared folder.
This function enables the operation to start on the control panel, through LAN lines (TopAccess) and according to the time.

- Start on the control panel
  When the E-FILING button is selected on the control panel to print, edit or delete the user document data saved in the Box or send the data by e-mail, the e-STUDIO starts this function.
  The e-STUDIO writes the user document data in the e-Filing Box in the work area of the HDD, outputs the data from the printer, saves the edited user document data or sends them by e-mail.

- Start through LAN lines (TopAccess)
  On the TopAccess screen, when printing, editing or deleting the user document data saved in the Box, sending the data by e-mail or archiving them or uploading their archives, the e-STUDIO starts this function.
  The e-STUDIO writes the user document data in the e-Filing Box in the work area of the HDD, outputs the data from the printer, saves the edited user document data in the e-Filing Box, sends them by e-mail or sends archives of the user document data to a PC (TopAccess).
  In addition, when uploading their archives from the PC (TopAccess), the e-STUDIO writes the received user document data in the work area of the HDD, and saves the data in the e-Filing Box.

- Start according to the time
  This function enables expired user data files saved in the e-Filing Box or shared folder to be deleted.

1.4.2.2 Security Function (Data Overwrite Function) in Normal Mode

There are two security functions in normal mode: Data Overwrite registration process and Data Overwrite process. These two functions are collectively called the Data Overwrite functions.

- Data Overwrite registration process
  Data Overwrite registration process starts when user document data are deleted in processing of (2) to (7) in 1.4.2.1 General Functions of the e-STUDIO in Normal Mode.
  This function overwrites registers the user document data with a deletion request (registers only its path). This function makes the deleted files targeted for Data Overwrite process.

- Data Overwrite process
  This function monitors the storage area of user document data to start and be deleted by Data Overwrite process after the power to the e-STUDIO is turned on, and permanently erases the area.
  While the user document data are being permanently erased, "ERASING DATA" appears on the control panel.

1.4.2.3 Settings for Maintenance/Device Information Display in Self-Diagnostic Mode

A service engineers starts and uses the self-diagnostic mode.

The settings for maintenance and device information display are divided into eight types listed in Table 1.4.2.3 Types of Self-Diagnostic Mode and their starting methods vary.

Some items of the "Setting" type affecting the security are described in 1.4.2.4 Security Functions in Self-Diagnostic Mode.

Type	Overview
Control Panel Check	Checks whether or not the panel LED lights up.
Tests	Checks the input signal status of LAN and USB lines.
Test Print	Prints a test pattern.
Adjustment	Adjusts hardware.
Setting	Set items.
List Print	Prints a list of counters.
PM Support	Resets counters.
Firmware Update	Updates system firmware.

Table 1.4.2.3 Types of Self-Diagnostic Mode

1.4.2.4 Security Functions in Self-Diagnostic Mode

In the "Setting" type in Table 1.4.2.3 Types of Self-Diagnostic Mode, a code is entered to start the functions after the e-STUDIO starts.

- Forcible Data Overwrite function
  This function is implemented on the control panel when the e-STUDIO is disposed of or the HDD is replaced.
  When this function is implemented, the remaining user document data in the HDD are collectively and permanently erased.

- Security License Registration/Deletion process
  The GP-1070 or GP-1140 is used to register or delete the license.
  When the security license is deleted, the e-STUDIO is unavailable. Installation of the TOE by the service engineer is required to restore the e-STUDIO.

- Type settings for HDD Overwrite/Forcible HDD Overwrite
  The overwrite types of Data Overwrite function in normal mode and forcible Data Overwrite in self-diagnostic mode are set.

1.4.3 Identification of Guidance Configuring the TOE

The guidance configuring the TOE is listed below:

Type	Identification No.	Document Name	Version	Remarks
Operator's Manual	OMJ080001C0	Safetly Infromation	Japanese Version	*1
	OME080002C0	Safety Information	English Version	
	OMJ08017500	e-STUDIO255/355/455 Quick Start Guide	Japanese Version	*2
	OME08017600	e-STUDIO205L/255/305/355/455 Quick Start Guide	English Version	
Service Manual	SMJ09000200	e-STUDIO255/355/455 Service Manual	Japanese Version	*3
	SME09000100	e-STUDIO205L/255/305 e-STUDIO355/455 SERVICE MANUAL	English Version	
	SHJ09000200	e-STUDIO255/355/455 Service Handbook	Japanese Version	
	SHE09000100	e-STUDIO205L/255/305 e-STUDIO355/455 SERVICE HANDBOOK	English Version	

*1 Request information to safely use this product

*2 Information on preparation for using this product and its basic usage

*3 Manual containing information required to maintain hardware/software for this product

Note: Only the guidance of the English version is to be evaluated because the e-STUDIO205L and e-STUDIO305 will not be marketed for Japan.

2. CONFORMANCE CLAIMS

This chapter describes reference to ST, reference to TOE and conformance to the CC.

2.1 Conformance Claims to the CC

Conformance to the CC that this ST and the TOE claim is described below:

CC Versions to which the ST and TOE claim conformance:

Part 1: Introduction and General Models, Version 3.1 Translated Version 1.2, March 2007
Part 2: Security Function Components, Version 3.1 Translated Version 2.0, March 2008
Part 3: Security Assurance Components, Version 3.1 Translated Version 2.0, March 2008

Conformance of ST to CC Version Part 2:	Conformance to CC Version Part 2
Conformance of ST to CC Version Part 3:	Conformance to CC Version Part 3

2.2 Protection Profile (PP) Claims, Package Claims

This ST conforms to the following evaluation assurance level and PP:

- The evaluation assurance level conforms to EAL3.
- There are no PPs to which this ST conforms.

2.3 Conformance Rationale

N/A.

3. SECURITY PROBLEM DEFINITION

This chapter defines security issues to be handled by the TOE and in its operating environment.

3.1 Threats

The details of potential attackers' threats against the e-STUDIO are described below:

- **T.TEMPDATA_ACCESS**
  A malicious user or unrelated user may attempt to retrieve user documents while surreptitiously removing the HDD from the e-STUDIO, restoring and decoding user document data deleted from the HDD of the e-STUDIO, using existing tools.

- **T.STOREDATA_ACCESS**
  A malicious user or unrelated user may attempt to retrieve user documents from the HDD disposed of or replaced of the e-STUDIO, using existing tools.

3.2 Organizational Security Policies

There are no organizational security policies for the TOE.

3.3 Assumptions

The assumptions for the TOE are described below:

- **A.TRUST_SE**
  It is assumed that the service engineer has knowledge required to operate the e-STUDIO in self-diagnostic mode and does not perform invalid operations.

- **A.NO_ERASE_STOP**
  It is not assumed that Data Overwrite process in normal mode is stopped due to power shutdown.

- **A.SECURITY_ENABLED**
  It is assumed that the e-STUDIO user and administrator use the TOE by making sure the security functions are running.

4. SECURITY OBJECTIVES

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

4.1 Security Objectives for the TOE

The security objectives for the TOE are described below:

- **O.TEMPDATA_OVERWRITE**
  The TOE needs to permanently erase user document data to be deleted from the HDD of the e-STUDIO, and delete the data in order to prevent them from being restored or decoded.

- **O.STOREDATA_OVERWRITE**
  The TOE needs to provide the capability to permanently erase all user document data in the HDD to be disposed of or replaced.

4.2 Security Objectives for the Operating Environment

The security objectives for the operating environment are described below:

- **OE.HDD_ERASE**
  The administrator requests the service engineer to dispose of or replace the e-STUDIO. The service engineer needs to permanently erase the HDD in order to prevent all user document data from being restored or decoded, when disposing of or replacing the e-STUDIO.

- **OE.TRUST_SE**
  The administrator needs to have the service engineer certified by Toshiba TEC Corporation operate the e-STUDIO in self-diagnostic mode. Toshiba TEC Corporation needs to have knowledge required by the service engineer, and ensures the service engineer does not perform invalid operations.

- **OE.NO_ERASE_STOP**
  The e-STUDIO user and administrator are not allowed to turn off the power to the e-STUDIO while "ERASING DATA" is displayed on the control panel in normal mode.

- **OE.SECURITY_ENABLED**
  The e-STUDIO user and administrator needs to make sure the security functions are running, on the control panel. When the security functions are not performed, they are not allowed to use the TOE.

Security Objectives Rationale

The table below shows the mapping of security objectives to assumptions and threats, and demonstrates every security objective for the TOE corresponds to at least one of the assumptions and threats.

	O.TEMPDATA_OVERWRITE	O.STOREDATA_OVERWRITE	OE.HDD_ERASE	OE.TRUST_SE	OE.NO_ERASE_STOP	OE.SECURITY_ENABLED
T.TEMPDATA_ACCESS	✓					
T.STOREDATA_ACCESS		✓	✓			
A.TRUST_SE				✓		
A.NO_ERASE_STOP					✓	
A.SECURITY_ENABLED						✓

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

- **T.TEMPDATA_ACCESS**
  O.TEMPDATA_OVERWRITE can counter threats, which may restore and decode the remaining magnetic data in the HDD, because user document data in the file deleted from the HDD of the e-STUDIO are permanently erased.

- **T.STOREDATA_ACCESS**
  O.STOREDATA_OVERWRITE can counter threats by preventing all user document data from being restored and decoded, because the forcible Data Overwrite function provides the capability to permanently erase the area of the user document data from the HDD of the e-STUDIO, **OE.HDD_ERASE** allows the administrator to request the service engineer to dispose of or replace the e-STUDIO, and the requested service engineer permanently erases the HDD.

- **A.TRUST_SE**
  OE.TRUST_SE satisfies the assumptions because Toshiba TEC Corporation ensures the certified service engineer has knowledge required to operate the e-STUDIO and does not perform invalid operations, and the administrator has the service engineer operate the e-STUDIO in self-diagnostic mode.

- **A.NO_ERASE_STOP**
  OE.NO_ERASE_STOP can satisfy the assumptions because the e-STUDIO user and administrator are not allowed to turn off the power while "ERASING DATA" is displayed on the control panel in normal mode, thus, Data Overwrite process is not stopped due to power shutdown.

- **A.SECURITY_ENABLED**
  OE.SECURITY_ENABLED can satisfy the assumptions because the e-STUDIO user and administrator do not use the TOE while the running security functions are not displayed on the control panel.

5. EXTENDED COMPONENTS DEFINITION

There are no extension components.

6. SECURITY REQUIREMENTS

This chapter describes the security requirements for the TOE.

6.1 TOE Security Functional Requirements

- FDP_RIP.1_TEMP Subset residual information protection_TEMP

  Hierarchical to: No other components

  Dependencies: No dependencies

  FDP_RIP.1_TEMP.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].

  List of objects

  1. The area to store the remaining user document data in the HDD when user documents are deleted during a job or when a job is finished
  2. The area to store expired user document data saved in the e-Filing Box or shared folder to be deleted

- FDP_RIP.1_ALL Subset residual information protection_ALL

  Hierarchical to: No other components

  Dependencies: No dependencies

  FDP_RIP.1_ALL.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].

  List of objects

  All existing user document data files in the HDD

6.2 TOE Security Assurance Requirements

The evaluation assurance level for the TOE is EAL3. The TOE security assurance requirement components are described below:

- Security Target evaluation
  - ASE_CCL.1 Conformance claims
  - ASE_ECD.1 Extended components definition
  - ASE_INT.1 ST introduction
  - ASE_OBJ.2 Security objectives
  - ASE_REQ.2 Derived security requirements
  - ASE_SPD.1 Security problem definition
  - ASE_TSS.1 TOE summary specification
- Development
  - ADV_ARC.1 Security architecture description
  - ADV_FSP.3 Functional specification with complete summary
  - ADV_TDS.2 Architectural design
- Guidance documents
  - AGD_OPE.1 Operational user guidance
  - AGD_PRE.1 Preparative procedures
- Life-cycle support
  - ALC_CMC.3 Authorisation controls
  - ALC_CMS.3 Implementation representation CM coverage
  - ALC_DEL.1 Delivery procedures
  - ALC_DVS.1 Identification of security measures
  - ALC_LCD.1 Developer defined life-cycle model
- Tests
  - ATE_COV.2 Analysis of coverage
  - ATE_DPT.1 Testing: basic design
  - ATE_FUN.1 Functional testing
  - ATE_IND.2 Independent testing - sample
- Vulnerability assessment
  - AVA_VAN.2 Vulnerability analysis

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirement Rationale

The table below shows the mapping of TOE security functions to security functional requirements, and demonstrates every TOE security function corresponds to at least one of the TOE security functional requirements.

	O.TEMPDATA_OVERWRITE	O.STOREDATA_OVERWRITE
FDP_RIP.1_TEMP	✓	
FDP_RIP.1_ALL		✓

The security functional requirements rationale is described below:

- **O.TEMPDATA_OVERWRITE**
  - **FDP_RIP.1_TEMP** (Subset residual information protection_TEMP)
    FDP_RIP.1_TEMP (Subset residual information protection_TEMP) disables the TOE to use any previous resource information when resources to delete files are deallocated, thus, TOE can permanently the area of user document data in the files deleted from the HDD of the e-STUDIO and **O.TEMPDATA_OVERWRITE** is satisfied.

- **O.STOREDATA_OVERWRITE**
  - **FDP_RIP.1_ALL** (Subset residual information protection_ALL)
    FDP_RIP.1_ALL (Subset residual information protection_ALL) permanently erases all user document data (objects) by operating the forcible Data Overwrite function and disables the TOE to use any previous resource information when the e-STUDIO is disposed of or the HDD is replaced, thus, **O.STOREDATA_OVERWRITE** is satisfied.

6.3.2 Security Assurance Requirements Rationale

The TOE is used in general office environments. Therefore, the opportunities of attack are limited and low attack capabilities of threat agents can be assumed regarding the TOE.
In order to counter the attacks by the threat agents, the coverage of security objectives, which must be analyzed during the development of TOE (systematic analysis and test of design, and security assurance of development environment), is to be evaluated.
Therefore, the appropriate evaluation assurance level for the TOE is EAL3.

7. TOE SUMMARY SPECIFICATION

This chapter describes the TOE summary specification.

7.1 Data Overwrite Function

The general functions of the e-STUDIO allow user document data temporarily generated and stored in the work area or stored in the e-Filing Box/shared folder, to deallocate resources when these storage areas are deleted.

- During a job started by the user or when it is finished
- The period to save data in the e-Filing Box or shared folder expires.

In this case, the TSF overwrites registers a path of the storage area, and uses the path erased and registered in the process where Data overwrite registration is monitored and the method to prevent the appropriate area from being reread out, to immediately overwrite and release the area. While data are being overwritten, "ERASING DATA" appears on the control panel.

The security functions (data overwrite functions) of the TOE are comprised of Data Overwrite registration process and Data Overwrite process.

Data Overwrite process overwrites 00, FF and random data in the storage area specified by the path and then releases the area, to permanently erase the area. The TOE allows this erase type to be used but more secure erase types to be selectable in self-diagnostic mode.

The Data Overwrite function can permanently erase the area of user document data and enables FDP_RIP.1_TEMP by preventing the area from being restored and decoded.

7.2 Forcible Data Overwrite Function

The TSF operates the forcible Data Overwrite function to overwrite all HDD storage areas including existing user document data files in the HDD with 00, FF and random data, and initialize the areas. This function ensures to prevent all areas of user document data from being restored and decoded, and enables FDP_RIP.1_ALL.