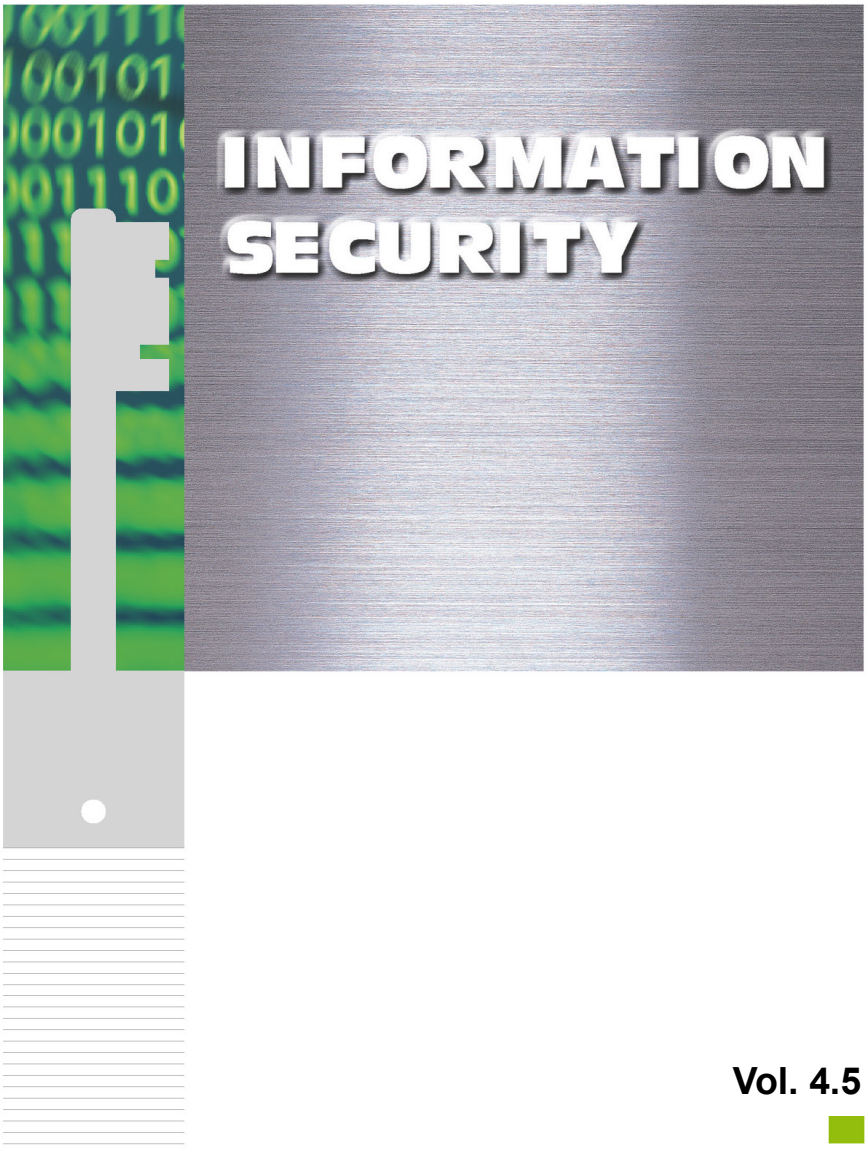
TOSHIBA

Leading Innovation



Vol. 4.5

Published by

Printing Solutions Business Group
TOSHIBA TEC CORPORATION

R13121304204-TTEC
OME150116C0

TABLE OF CONTENTS

TRADEMARKS AND COPYRIGHT

Trademarks

- Windows, and the brand names and product names of other Microsoft products are trademarks of Microsoft Corporation in the US and other countries.
- Mifare is a trademark of NXP Semiconductors.
- Acrobat is a trademark of Adobe Systems Incorporated in the US and other countries.
- Other company names and precuts names in this document are the trademarks of their respective companies.

Copyright

1. ENTIRE POLICY

1.1. Security Technology Roadmap

Protection Assets	Threats	Countermeasures (Security Functions)	
Residual data of the user document	(1) Leakage of information due to a theft of the HDD	AES (Advanced Encryption Standard) Encryption Chip on Board	
		Delete all data in the HDD when destroying	
		Erase automatically after copying/printing/scanning is completed (Data Overwrite Kit)	
		Guarantee of Encryption Module (Compliant to FIPS 140-2)	
		ADI HDD (Wipe Technology HDD)	
Confidential Document Data	(2) Unauthorized access from the control panel or the Web, spooling, data theft, falsification/wiretapping	Password authentication (BOX password)	
		User authentication function	Windows Authentication
			LDAP authentication
			Role-Based Access Control
			Restrict Service technician to access
			Password Policy
			Restrict Scan Destination
			IC card (FeliCa)
			IC card (MIFAREIHID)
			Support Multiple IC Card
			Single Sign On
			Confidentiality of the name of document
	(3) Unauthorized access from the network, spooling, data theft, falsification/wiretapping	Close unnecessary port	
		Port Filtering	IP Address Filtering
			MAC Address Filtering

	(4) Unauthorized copy	Hardcopy Security Printing	Hardcopy Security Printing (Control Copying)
			Hardcopy Security Printing (Prohibit Copying/Info. Tracking)
	(5) Taking Away Prevention	Private Printing	
		Hold Printing (Print, FAX/iFAX, Email)	
	(6) Unauthorized email	User authentication function	POP before SMTP
			SMTP authentication
			LDAP authentication
	(7) Data wiretapped over the network	SSL/Server authentication (eBDM)	
		SSL/TLS	SMTP, POP3, LDAP, IPP, DPWS (Print, Scan), FTP,HTTP
		IPsec	
		IEEE 802.1X	
		Digital Certificate	PKI
			SCEP
		SNMPv3	
		SNTP Authentication	
		Secure DDNS	
	(8) Data wiretapped over the wireless LAN	WPA/WPA2 compliant	
		IEEE 802.1X	
	(9) Leakage of electronic file	Encrypted PDF	
	(10) Miss-Fax sending to other destination	Prevention from FAX miss-sending to other destination	
	(11) Unauthorized access from the telephone line	Communication cut other than FAX protocol	
Job Log, Address Book	(12) Unauthorized access from the control panel or the Web	Administrator privilege: password authentication	
		User privilege: password authentication	
		Log records whether copying/printing/scanning by user succeeded or failed	
		Restriction of editing Address Book	
		Record various Security Log	
		Access Restriction to Log	

All Data	(13) Illegal Access	Software Falsification Prevention	
		Firewall	
		Unnecessary Service Stop	
		Encryption of Firmware Data/Prevention of Falsification	
		High Security Mode	
		Encryption of Cloning Data/Prevention of Falsification	
	(14) Industry Standard	Compliant to IEEE 2600.1 (MFP Security Standard)	e-STUDIO2040C/2540C/3040C/3540C/4540C, e-STUDIO5540C/6540C/6550C, e-STUDIO206L/256/306/356/456/506, e-STUDIO556/656/756/856, e-STUDIO2050C/2550C, e-STUDIO2555C/3055C/3555C/4555C/5055C, e-STUDIO306LP, e-STUDIO5560C/6560C/6570C, e-STUDIO207L/257/307/357/457/507, e-STUDIO557/657/757/857, e-STUDIO2000AC/2500AC, e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC, e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A, e-STUDIO5506AC/6506AC/7506AC, e-STUDIO5508A/6508A/7508A/8508A
		Compliant to IEEE 2600.2 (MFP Security Standard)	e-STUDIO3508LP/4508LP/5008LP
		Support Encryption Y2010 Problem	

1.2. Security Technologies

1.2.1. Protection of HDD Data

1. Function Summary

The function is to protect data written temporarily onto the HDD.

The HDD (hard disk device) is equipped in the MFP (Multi Function Peripheral). Original document data from scanning operations, such as copying, is stored temporarily in the HDD. When copying is completed, although the management information (FAT: File Allocation Table) is erased, the temporarily stored data still remains in the HDD. In addition, a confidential document can be stored and controlled with a password in a Filing Box of the HDD.

Some people may be concerned that if a person with bad intent steals the HDD, the person can recreate a document from residual data or data in a Filing Box and may be able to steal confidential and private information. By utilizing the following encryption function and data overwriting function, the HDD data can be protected.

2. Current Approach

The e-STUDIO2500C/3500C/3510C, e-STUDIO2330C/2830C/3520C/4520C, e-STUDIO5520C/6520C /6530C, e-STUDIO255/355/455, e-STUDIO655/755/855, e-STUDIO2040C/2540C/3540C/4540C, e-STUDIO5540C/6540C/6550C, e-STUDIO256/306/356/456/506, e-STUDIO556/656/756/856, e-STUDIO5560C/6560C/6570C, e-STUDIO207L/257/307/357/457/507, and e-STUDIO557/657/757/857 have a HDD encryption feature as standard equipment, allowing written data on the HDD to be encrypted using an AES (Advanced Encryption Standard) 128-bit algorithm. AES is a U.S. government-approved cryptographic algorithm that is recommended by the National Institute of Standards and Technology (NIST).

Installation of an optional data overwrite kit (GP-1060/1070) allows data temporarily stored on the HDD from a copying, printing, scanning or faxing operation to be automatically overwritten and erased after the operation is completed. This data overwrite kit also has a function to completely erase the data in all HDD areas. A service engineer performs this function according to the customer's instructions. Therefore, the retrieval of residual data on the HDD is completely disabled. This data overwrite kit also has a function to completely erase the data in all HDD areas. A service engineer performs this function according to the customer's instructions. Therefore, the retrieval of residual data on the HDD is completely disabled.

In addition, Security HDD, which is installed in the e-STUDIO2040C/2540C/3040C/3540C/4540C, e-STUDIO5540C/6540C/6550C, e-STUDIO206L/256/306/356/456/506, e-STUDIO556/656/756/856, e-STUDIO2050C/2550C, e-STUDIO287CS/347CS/407CS, e-STUDIO477S/527S, e-STUDIO2555C/3055C/3555C/4555C/5055C, e-STUDIO306LP, e-STUDIO5560C/6560C/6570C, e-STUDIO207L/257/307/357/457/507, e-STUDIO557/657/757/857, e-STUDIO2000AC/2500AC, e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC, e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A, e-STUDIO5506AC/6506AC/7506AC, e-STUDIO5508A/6508A/7508A/8508A and e-STUDIO3508LP/4508LP/5008LP encrypts all data on the HDD using an AES 256-bit algorithm. Therefore, even if the HDD is stolen, data invalidation works to prevent information leaks as soon as the HDD is installed in another device, and an attempt is made to illegally read data out of the HDD. After completion of the use of the multifunction peripheral (MFP) or at the end of the lease period, all data on the HDD is instantly invalidated and data retrieval is completely disabled, once the service engineer operates the MFP according to the customer's instructions.

e-STUDIO2040C/2540C/3040C/3540C/4540C, e-STUDIO5540C/6540C/6550C, e-STUDIO206L/256/306/356/456/506, e-STUDIO556/656/756/856, e-STUDIO2050C/2550C, e-STUDIO287CS/347CS/407CS, e-STUDIO477S/527S, e-STUDIO2555C/3055C/3555C/4555C/5055C, e-STUDIO306LP, e-STUDIO5560C/6560C/6570C, e-STUDIO207L/257/307/357/457/507, e-STUDIO557/657/757/857, e-STUDIO2000AC/2500AC, e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC,

e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A, e-STUDIO5506AC/6506AC/7506AC e-STUDIO5508A/6508A/7508A/8508A and e-STUDIO3508LP/4508LP/5008LP for North America are equipped with a Security HDD validated to the FIPS 140-2 standard. For other regions, the Security HDD validated to the FIPS 140-2 standard is provided as an option.

SSD is installed in e-STUDIO2051C/2551C and e-STUDIO2050C/2550C has an encryption feature as standard, and the data inside of SSD is encrypted by AES 128-bit algorithm. After completion of the use of the MFP or at the end of the lease period, a service engineer initializes the SSD according to the customer's instructions.

These functions are certified by ISO/IEC15408 (Common Criteria), which is an international standard for information security.

Combination		Acquisition
Equipment	Option	
e-STUDIO550/650/810	GP-1010	EAL2 certified in March 2004
e-STUDIO3511/4511	GP-1031	EAL2 certified in March 2005
e-STUDIO600/720/850	GP-1060	EAL3 certified in March 2006
e-STUDIO281C/351C/451C		
e-STUDIO232/282		
e-STUDIO352/452		
e-STUDIO2500C/3500C/3510C	GP-1060	EAL3 certified in June 2006
e-STUDIO600/720/850	GP-1060	EAL3 certified in August 2008
e-STUDIO232/282		
e-STUDIO352/452		
e-STUDIO2330C/2830C/3520C/4520C	GP-1070	EAL3 certified in December 2008
e-STUDIO5520C/6520C/6530C		
e-STUDIO255/355/455	GP-1070	EAL3 certified in June 2009
e-STUDIO655/755/855		
e-STUDIO2040C/2540C/3040C/3540C/4540C	GP-1070	Compliant to IEEE 2600.1 EAL3+ certified in October 2011
e-STUDIO5540C/6540C/6550C		
e-STUDIO206L/256/306/356/456/506	GP-1070	Compliant to IEEE 2600.1 EAL3+ certified in May 2012
e-STUDIO556/656/756/856		
e-STUDIO2050C/2550C	GP-1070	Compliant to IEEE 2600.1 EAL3+ certified in October 2012
e-STUDIO2555C/3055C/3555C/4555C/5055C	GP-1070	Compliant to IEEE 2600.1 EAL3+ certified in April 2013
e-STUDIO306LP	GP-1070	Compliant to IEEE 2600.1 EAL3+ certified in November 2013

e-STUDIO5560C/6560C/6570C e-STUDIO207L/257/307/357/457/507 e-STUDIO557/657/757/857	GP-1070	Compliant to IEEE 2600.1 EAL3+ certified in November 2015
e-STUDIO2000AC/2500AC e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A	GP-1070	Compliant to IEEE 2600.1 EAL3+ certified in September 2016
e-STUDIO5506AC/6506AC/7506AC e-STUDIO5508A/6508A/7508A/8508A	GP-1070	Compliant to IEEE 2600.1 EAL3+ certified in November 2016
e-STUDIO3508LP/4508LP/5008LP	GP-1070	Compliant to IEEE 2600.2 EAL2+ certified in July 2017

1.2.2. Confidential Document Access Restrictions

1. Function Summary

Regarding an image stored in the HDD, access restriction must be password authenticated. Image data that needs to be handled as a confidential document will be protected from leakage and falsifications by a third party.

2. Current Approach

Filing Box with a Password

Setting a 64-digit password into the HDD of the MFP can create a Filing Box. The file stored in the filing box can be printed from the control panel. Thumbnail display from a client PC Web browser and editing can be access restricted by the password. A box password can be applied to the password policy.

Secure Print Function

With invalid user authentication, private print is used to transmit print data with a password up to 64 alphanumeric characters from the client PC to the MFP, the transmitted data is accumulated temporarily onto the HDD of the MFP. Unless the password is entered on the control panel, printing does not start.

With user authentication in use, hold print or private print is used to allow users to command only print jobs sent on their own without entering a password for private print, after logging into the MFP. By setting the MFP to require a user name and password when a job is sent to the MFP from the printer driver, user authentication is available for a shared PC used by multiple users.

In addition, users can command their own print jobs by simply holding an IC card over the control panel instead of performing user authentication, through the use of an optional authentication non-contact IC card device, HID/Mifare, etc. Once logged in, users are also allowed to automatically output their print data without sending a print job.

Secure print can be switched to forced private print or forced hold print.

The filing box with a password or private print/hold print function is used to store or print confidential documents.

The administrator configuration allows all jobs to be temporarily stored in private or hold queues, and then released as desired, instead of being immediately released.

Document or user names can be hidden on the status screen to ensure security.

Encrypted PDF

This function is available to encrypt PDF documents and restrict the operation by setting a password during scanning. Encryption is applied to secret key cryptography, ‘RC4’. Entering the password (user password) can display the encrypted PDF document. An encryption level can be selected from 128-bit RC4 compatible with Acrobat 5.0 and PDF V1.4, 40-bit RC4 compatible with Acrobat 3.0 and PDF V1.1, and 128-bit AES compatible with Acrobat 7.0 and PDF V1.6. Operation restrictions can be set for Print, Documents Change, Contents Extraction and Accessibility, respectively. The restriction setting information is protected by password (master password).

If the encrypted PDF document is sent to a wrong destination or sniffed, this function prevents users who do know the password from viewing the document. This function also protects distributed PDF documents from unauthorized printing or tampering.

Confidential Setting of Document Name

This function allows to indicate a document name, a user name and a destination by “*” when a job state or log is displayed on the touch panel or TopAccess.

1.2.3. User Authentication Function

1. Function Summary

A user authentication function is equipped in the MFP in order to prevent unauthorized access to the MFP. The user authentication function provides the following user management tasks:

- Restrict operations on the touch panel
- Restrict access to device configuration or log information
- Restrict available operations (copying/printing/scanning/faxing) by user. (Role-Based Access Control)
- Log operations by user
- Manage the counter by user
- Necessity/unnecessity setting of user authentication at each function

2. Current Approach

Restriction on operation by user authentication

Operations on the touch panel can be restricted by first having an authentication screen displayed. It is possible to set whether the authentication screen is to be displayed or not when each function button (COPY, SCAN, PRINT, and FAX) is pressed by setting the user authentication for each function of the MFP.

Registration and management of user information

1) Regarding department management, up to 1,000 departments can be registered and used. Also, up to 10,000 users can be registered in the MFP.
2) It can be coordinated with the user authentication system established in the corporation. Available user authentication systems are the Windows authentication system (Active Directory) that is generally widely used directory services, and LDAP. As for authentication method, in addition to entering an ID and password on the keyboard, a non-contact IC card, HID/Mifare etc., which provides both convenience and security, can be used as an optional authentication device. This authenticates a user and allows him/her to use the MFP just by holding a HID/Mifare card onto the card reader connected to the MFP, eliminating a cumbersome password entry on the control panel. Also, as the existing corporate ID card (HID/Mifare, etc.) used to enter/leave a room can be used for operating the MFP without making any changes, this method can be introduced at low cost.

   According to this enhanced password policy, a strong password can be set in local authentication.

1.2.4. Role-Based Access Control

1. Function Summary

Unauthorized usage of the MFP may cause information leakage from a copying, printing, scanning or filing box operation. To prevent the leakage, available operations by user can be restricted. Enabling the user authentication function and Role-Based Access Control function is required in order to use this function.

2. Current Approach

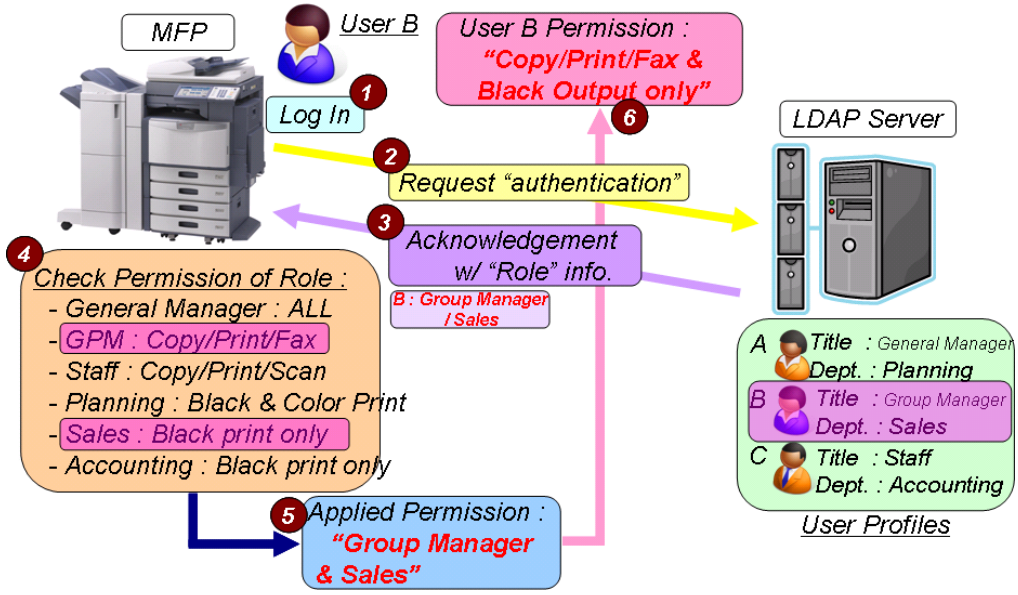
After user authentication is completed through the control panel or TopAccess, operations (objects) that are only permitted are copying/printing/faxing/monochrome output is available, while scanning/color output is prohibited for Person B.

Setting of Role for each user (which means the role of each user, and which is able to set for the administrator or the general user, or belonging section.) is available in the centralized managed directory database LDAP (including the Active Directory LDAP function). And Role, which LDAP server has already had beforehand, is utilized also.

When logging in MFP with user authentication function, MFP acquires the Role information, which has already been allocated in LDAP server, and checks the right of access (Access Control List: ACL) to MFP, which is allocated in its Role, and gives a permission of usage for each functionality to a user. The following ten settings are available for the rights of access to be allocated in Role.

Device setting, Copy, E-mailSend, FileSave, iFaxSend, Print, e-Filing, FaxSend, Color output (Copy/Print), Remote Scan, USB Print/Save, Editing Address Book, Log management can be set. As the setting of Role information can be allocated the access right to all users attributes set in the existing LDAP Server, a new LDAP Server is not required, and you can set it securely.

In addition, roles will be set in local authentication or created by the administrator.



1.2.5. Network Access Restrictions

1. Function Summary

MFP has a TCP/UPD port opened in order to provide a network service. A client PC is connected to the MFP port that could respond to the service via the network.

For example, in order to provide the LPD printing service, the 515 port of the MFP is opened. Some customers may be concerned that if an unnecessary port is opened, it can become a security hole.

2. Current Approach

A port, which does not provide a service, is not opened. An unnecessary port for operation can be closed by an administer restriction.

1.2.6. IP/MAC Address Restrictions

1. Function Summary

Only an access request from a network node (PC, etc.) with an IP address registered in the MFP is accepted.

This will restrict access from a malicious network node.

2. Current Approach

Both IP Address Filtering and MAC Address Filtering are supported. And both functions which accept an access request only from a PC with a specific IP address or MAC address registered in the MFP, and which does not accept an access request from a PC with a specific IP address or MAC address registered in the MFP, are supported.

In the following models, the filtering will be set by each port. In addition, responding/non-responding to ICMP can also be set.

e-STUDIO2000AC/2500AC, e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC,
e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A, e-STUDIO5506AC/6506AC/7506AC,
e-STUDIO5508A/6508A/7508A/8508A, e-STUDIO3508LP/4508LP/5008LP

1.2.7. Hardcopy Security Printing

1. Function Summary

Embedded pattern print is a security function, which effectively restricts or prohibits unauthorized copying and prevents the leakage of information printed on hardcopy, when a particular fine dot pattern is embedded during printing. If the hardcopy information is leaked outside, it can be traced through analysis of the embedded pattern later.

To prevent the leakage of information printed on the document or unauthorized copying of a confidential document, only adding a particular embedded pattern to the document by pre-embedding hidden character strings such as “Copying Prohibited” makes the embedded pattern appear conspicuously on the document when it is copied. It is intended to effectively restrict unauthorized copying.

To prohibit unauthorized copying, adding an embedded pattern to the printed matter disables copying, scanning or faxing of the matter when any attempt is made. This ensures the strict protection of the confidential document.

If the printed matter is left unattended, by scanning the matter and analyzing its embedded pattern with optional software, the source where the information (data) was created is identified, which helps with the management of confidential documents.

2. Current Approach

If restricting unauthorized copying is required, changing the setting by requesting a service engineer and specifying Hardcopy Security Printing on a client PC to print a document will incorporate an embedded pattern (fine dot pattern). When this printed document is copied, pre-embedded character strings such as “Do Not Copy” or “Copying Prohibited” will appear conspicuously to restrict information leakage due to unauthorized copying.

On the optional device (GP-1190A) for the e-STUDIO2040C/2540/3040C/3540C/4540C, e-STUDIO5540C/6540C/6550C,e-STUDIO2050C/2550C* e-STUDIO2555C/3055C/3555C/4555C/5055C, e-STUDIO5560C/6560C/6570C, e-STUDIO2000AC/2500AC, e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC and e-STUDIO5506AC/6506AC/7506AC, if restricting unauthorized copying is required, specifying Hardcopy Security Printing on a client PC when printing a document will incorporate an embedded pattern (fine dot pattern). When this printed document is copied, pre-embedded character strings such as "COPY" will appear conspicuously to restrict information leakage due to unauthorized copying. Any attempt made to copy, fax or scan printed matter on a Toshiba MFP equipped with a copy prohibit function will result in the disabling of copying, scanning or faxing. If the printed matter is left unattended, by analyzing the image data from which the printed matter was scanned, information on the creation and printing of the printed matter, such as "when," "who," "what," "which PC to create" and "which MFP to print," is retrieved and displayed on the PC screen.

*. If optional Hardcopy Security Printing Kit (GP-1190A) is used in e-STUDIO2050C/2550C, optional HDD (GE-1220/C) is required.

1.2.8. Security Function during E-mail Transmission

1. Function Summary

Unauthorized usage of the Scan-To-E-mail function may cause information leak through E-mails or wiretapping. To prevent this problem, Scan to E-mail function provides the security function for E-mail transmission.

2. Current Approach

The following security functions are supported for e-mail transmission in Scan to E-mail function of the MFP.

1) User authentication
   As the authentication systems, standard protocols (POP before SMTP, SMTP Authentication (LOGIN/PLAIN/CRAM-MD5/Digest-MD5/Kerberos) and LDAP Authentication (LOGIN/PLAIN/CRAM-MD5/Digest-MD5/Kerberos) are equipped in the MFP, thus, the protocols can be selected in accordance with the corporate policy.

2) Encryption

   Encryption (SMTP SSL/TLS) of the communication path during E-mail transmission is supported to prevent wiretapping of E-mails on the network.

3) BCC transmission function

   The Bcc (Blind Carbon Copy) function is also available for transmitting internet faxes as well as the email transmission.

1.2.9. Communication Protection (Wired)

1. Function Summary

Encrypted communication that flows over the network can protect communications. Although communication data can easily be wiretapped when the Network Trace Tool is used, through encryption, it will not be stolen even when wiretapped.

1.2.9.1. SSL (Secure Socket Layer)/TLS (Transport Layer Security)

1. Function Summary

Protocol to be sent/received with data encrypted over the network which was developed in Netscape Communications Inc. Encryption in combination with open key encryption, confidential key encryption, digital certificate, and hash function can prevent wiretapping of data, falsification, and unauthorized usage. TLS V1.0 is improved slightly based on SSL 3.0, and is standardized for RFC2246 in IETF.

2. Current Approach

SSL/TLS communication is supported in HTTP Server/Client, IPP, LDAP, SMTP Client, POP3, FTP Server, Web Service Print, FTP Client and Web Services Scan.

For the HTTP Server function, within the Remote Device Management System (RDMS), the MFP administration information is transmitted to the Internet server, to carry out SSL/TLS encryption. SSL/TLS encryption is also carried out for access to TopAccess. Communication via HTTP and SSL/TLS is used for access to the Address Book Viewer.

In IPP SSL, SSL/TLS encryption prevents print data from being wiretapped.

In POP3/SMTP, SSL/TLS communication prevents e-mail data from being wiretapped.

The FTP server function is used to backup/restore FTP print data and e-Filing Box data. SSL/TLS encryption can prevent these data from being wiretapped.

In Web Service Print, SSL/TLS encryption can prevent print data from being wiretapped.

In Web Service Scan and TWAIN Scan, SSL/TLS encryption can prevent data via Remote Scan from being wiretapped.

In FTPS, communications in Scan to Remote can be encrypted.

This MFP supports POODLE and FREAK. Therefore, a lower security encryption / transmission system such as SSL2.0/3.0 or SHA-1 is not used.

1.2.9.2. IPsec (IP Security Protocol)

1. Function Summary

IPsec (IP Security Protocol) protects communication in IP layer. It is said that the person who sends/receives data is authenticated, and non-repudiation is protected in order to secure confidentiality and entirety.

2. Current Approach

Both AH (Authentication Header) and ESP (Encapsulating Security Payload) security protocols are supported. AH secures entirety of IP Packet, and ESP secures confidentiality and entirety of IP Packet. For Key management protocol together with IPsec used, IKEv1 and IKEv2 are supported. Import or SCEP can be utilized in order to install the certificate. IPv6 Readylogo for IPsec is also supported, and IPsec Ready Logo Phase-II is corresponded.

1.2.9.3. Wired IEEE802.1X

1. Function Summary

IEEE802.1X is a standard for authentication utilized in LAN connecting. As IEEE802.1X is known well for user authentication specification in wireless LAN such as IEEE802.11b, specification itself is correspondent to wired LAN. It consists of supplicant, 802.1X switch, and authentication server. IEEE802.1X does not accept all communication from clients who are not certified, but it does accept communication from users to be certified. EAP (Extensible Authentication Protocol) is used to transmit an authentication message. EAP authentication has EAP-MD5 and EAP-TLS methods.

2. Current Approach

There are some EAPs to be utilized in 802.1X, and both supplicant and authentication server need to be correspondent to EAPs. Currently EAP-MD5, MSCHAPv2, EAP-TLS, EAP-TTLS, and PEAP are supported. In installation of the certificate with EAP-TLS, EAP-TTLS, and PEAP used, Import or SCEP can be utilized.

1.2.9.4. Network Authentication

LDAP authentication supports CRAM-MD5, Digest-MD5 and Kerberos to protect the username and password required for access to the LDAP server.

SMTP authentication supports CRAM-MD5, Digest-MD5, Kerberos and NTLM (IWA: Integrated Windows Authentication) to protect the username and password required for access to the SMTP server.

POP3 authentication supports Kerberos, NTLM (SPA: Secure Password Authentication) and APOP to protect the username and password required for access to the POP3 server.

SMB authentication supports NTLMv2 and Kerberos.

Dynamic DNS supports Secure Dynamic DNS (Domain Name System). When Secure Dynamic DNS is used, only the MFP in which the resource record was registered or device with management authority for the DNS server can update zone information.

SNTP supports SNTP authentication, enabling authentication of an SNTP session between the MFP and SNTP server.

1.2.9.5. SNMPv3

Network Protocol SNMPv3, which has both data encryption and user authentication function, enhances security features.

1.2.10. Communication Protection (Wireless)

1. Function Summary

This function encrypts wireless communication to prevent decryption and access by a third party. It can also allow communications only with a pre-permitted party when a connected party is authenticated.

Since wireless communication is performed by radio waves, communication could be intercepted in radio waves service areas.

To prevent unauthorized usage by the third party, such as a falsification of data and spoofing, a wireless LAN option supports WPA and the next-generation-standard, WPA2, which encrypts communication data and allows user authentication for a communication party.

2. Current Approach

WPA and WPA2 are security standards established by Wi-Fi Alliance. WPA was created as a subset of IEEE802.11i, especially for improving user authentication and encryption. Later on, WPA2 that completely complies with IEEE802.11i was released. Compared with WPA, WPA2 provides more enhanced encryption and connectivity.

Two connection methods are supported, as follows.

WPAPSK allows user authentication and encrypts data when a "passphrase" shared between an access point and a client PC is preset. "Passphrase" is an optional character string set with from 8 to 63 characters. In addition to WPAPSK, a stronger security system (802.1X authentication) through a RADIUS server (authentication server) is supported. This is a connection mechanism, which verifies if the connected access point and the client PC are mutually appropriate parties.

As 802.1X authentication systems, EAP-TLS with a digital certificate and PEAP with a password are supported.

To make 802.1X authentication faster, WPA2 optionally supports Pairwise Master Key (PMK) caching. PMK caching stores an authentication result including an encryption key to connect to a wireless LAN access point smoothly even if the location is changed.

1.2.11. Telephone Line Access Restriction

1. Function Summary

There are MFPs with a FAX function.

Since these types of machines connect directly to the telephone line, some people are concerned that the data in the MFP may be stolen by making a dial-up connection.

For the customers using the Remote Diagnosis Configuration, they may worry about the registered data being leaked.

2. Current Approach

Regarding telephone line access, the MFPs do not accept another protocol, only the FAX. The current FAX board only supports a standard G3FAX and the unique procedural protocol (*) of Toshiba. When you connect with someone having a device other than a regular FAX or a Toshiba FAX, the protocol cannot be established. As a result, it becomes a communication error and the line disconnects. Therefore, you will not be able to access the network through a FAX board from a telephone line. Furthermore, there is no chance of improper data becoming mixed.

Remote-Maintenance from FAX line is not supported.

* There is an abbreviated protocol, which is a unique procedure utilized only by Toshiba.

1.2.12. Log Information Access

1. Function Summary

Operations on the control panel and in TopAccess can be recorded as logs in order to prevent unauthorized usage of the MFP and ensure traceability.

2. Current Approach

By enabling user authentication, whether operations (copying/printing/scanning/fax transmitting and receiving) by the user succeed or fail can be logged. Thus, unauthorized access or fraud can be detected. On the control panel or in TopAccess, obtained logs can be observed. When user authentication is enabled, users can browse only their own job logs.

When user authentication is disabled, job logs can be switched between visible and hidden, allowing administrators and auditors to browse all logs.

Various security logs are added.

SYSLOG has also been supported in e-STUDIO2000AC/2500AC,
e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC,
e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A, e-STUDIO3508LP/4508LP/5008LP.

1.2.13. Tracking

1.2.13-1. Tracking by Image Log

1. Function Summary

To ensure the traceability of the MFP's copying/scanning/faxing data, they can be stored as image thumbnail data along with the job information.

2. Current Approach

When copying/scanning is performed or a fax is transmitted or received in the MFP, the data can be transmitted to a designated external server as the image thumbnail data along with the job information (date and time, user name, file name, serial number of the MFP). This function enables the tracking of data if an information leak occurs due to copying/scanning/faxing with the MFP.

To prevent information leak by improperly utilizing this function, it is disabled by default. The service engineer needs to enable this function to use it.

1.2.13-2. Tracking by Forced Printing

1. Function Summary

To enable the tracing of the MFP's copying/printing documents, information such as the date and time, user name, etc. can be forcibly printed onto them.

2. Current Approach

Forced printing of the date and time, user name and card ID enables the tracking of the data as to who has performed output copying, printing and fax transmission as well as when.

1.2.14. E-Mail

1. Function Summary

Since the MFP has an E-mail receiving function, customers may worry about virus infections when receiving E-mail.

2. Current Approach

The E-mail receiving function is equipped in the MFP and is classified into 3 main functions:

1) Printing received mail content and an attached image.
2) Storing an attached image from received mail into the e-Filing Box.
3) FAX transferring of an attached image from received mail (Off Ramp function).

These mail-receiving functions do not have the ability to process even if a program language is described. Therefore, a received malicious program will not be executed. The only attached file that can be printed is a TIFF file, which does not have any macro function.

Off Ramp function can restrict telephone numbers. Therefore, a telephone call cannot be made to a selected telephone number.

POP3 and SMTP protocol, which encrypts data in SSL/TLS, prevents mail data from being wiretapped.

1.2.15. Response to Network Viruses

1. Function Summary

Customers may be concerned about infection of network viruses (worms) targeted at MS Windows such as MSBLAST, or infection from websites (TopAccess) targeting MFPs. They may be also concerned about countermeasures against viruses that invade MFPs via USB.

2. Current Approach

MFPs are not affected by network viruses targeted at MS Windows. Existing website vulnerabilities include Cross-Site Request Forgery (CSRF), Cross Site Scripting (XSS) and SQL Injection, and MFPs have taken measures to address these vulnerabilities, as well as for viruses, which invade MFPs via USB. Security patches will be available as needed. MFPs have also taken measure to the vulnerabilities such as OpenSSL POODLE vulnerability, FREAK vulnerability in the SSL/TLS communication, GHOST, Heartbleed, and Shellshock.

1) Response to viruses in OS

VxWorks for integration of computers developed by Wind River is incorporated into the previous MFPs, such as the e-STUDIO2330C/2830C/3520C/4520C, e-STUDIO5520C/6520C/6530C, and e-STUDIO255/355/455, e-STUDIO655/755/855 in the OS. The MFPs are therefore not infected with viruses or worms originating in MS Windows, nor does the system go down due to viruses. VxWorks has been widely introduced in aerospace and defense fields where high reliability and safety are required. No security holes or vulnerabilities have been reported, thus, unlike MS Windows, no periodic application of security patches is required.

Open Source Linux is incorporated into the MFPs OS, such as the e-STUDIO2040C/2540C/3040C/3540C/4540C, e-STUDIO5540C/6540C/6550C, e-STUDIO206L/256/306/356/456/506, e-STUDIO556/656/756/856, e-STUDIO2050C/2550C, e-STUDIO2051C/2551C, e-STUDIO287CS/347CS/407CS, e-STUDIO477S/527S, e-STUDIO2555C/3055C/3555C/4555C/5055C, e-STUDIO306LP, e-STUDIO5560C/6560C/6570C, e-STUDIO207L/257/307/357/457/507, e-STUDIO557/657/757/857, e-STUDIO2000AC/2500AC, e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC, e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A, e-STUDIO5506AC/6506AC/7506AC and e-STUDIO5508A/6508A/7508A/8508A. The MFPs are therefore not infected with viruses or worms originating in MS Windows, nor does the system go down due to viruses.

Security patches will be available as needed.

2) Response to viruses from websites

a) Cross-Site Request Forgery (CSRF)

Previous MFPs, such as the e-STUDIO2330C/2830C/3520C/4520C, e-STUDIO5520C/6520C/6530C, and e-STUDIO255/355/455, e-STUDIO655/755/855 implemented CSRF(Cross-Site Request Forgery) to access the page to be processed using the POST method, to automatically generate a previous page, allowing confidential data to be inserted into the hidden parameter, and to process the page only when the value on the page to be processed is correct. Thus, the MFPs never cause vulnerabilities.
Session management is supported for e-STUDIO2040C/2540C/3540C/4540C, e-STUDIO5540C/6540C/6550C, e-STUDIO206L/256/306/356/456/506, e-STUDIO556/656/756/856, e-STUDIO2050C/2550C, e-STUDIO2051C/2551C, e-STUDIO287CS/347CS/407CS, e-STUDIO477S/527S, e-STUDIO2555C/3055C/3555C/4555C/5055C, e-STUDIO306LP, e-STUDIO5560C/6560C/6570C, e-STUDIO207L/257/307/357/457/507, e-STUDIO557/657/757/857, e-STUDIO2000AC/2500AC, e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC, e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A, e-STUDIO5506AC/6506AC/7506AC e-STUDIO5508A/6508A/7508A/8508A and e-STUDIO3508LP/4508LP/5008LP. And a session is

discarded after a timeout or logout. In addition, the session retention time can be set in TopAccess.

b) Cross Site Scripting (XSS)

Previous MFPs, such as the e-STUDIO2330C/2830C/3520C/4520C, e-STUDIO5520C/6520C/6530C, and e-STUDIO255/355/455, e-STUDIO655/755/855 used JavaScript to strictly monitor input data from a web client when it is set or entered in TopAccess, disabling the MFPs from saving data. After checking is finished on the server where the program evaluates values, the MFPs then write them into SRAM.

Escape processing is enabled for MFPs, such as the e-STUDIO2040C/2540C/3540C/4540C, e-STUDIO5540C/6540C/6550C, e-STUDIO206L/256/306/356/456/506, e-STUDIO556/656/756/856, e-STUDIO2050C/2550C, e-STUDIO2051C/2551C, e-STUDIO287CS/347CS/407CS, e-STUDIO477S/527S, e-STUDIO2555C/3055C/3555C/4555C/5055C, e-STUDIO306LP, e-STUDIO5560C/6560C/6570C, e-STUDIO207L/257/307/357/457/507, e-STUDIO557/657/757/857, e-STUDIO2000AC/2500AC, e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC, e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A, e-STUDIO5506AC/6506AC/7506AC e-STUDIO5508A/6508A/7508A/8508A and e-STUDIO3508LP/4508LP/5008LP to monitor input symbols and characters ("|", "<" and ">"), which are more likely to be used for command injection attacks when an illegal command is entered in the OS (Linux). JavaScript is used to strictly monitor input data from a web client when it is set or entered in TopAccess, disabling the MFPs from saving data. After checking is finished on the server where the program evaluates values, the MFPs then write them into SRAM.

c) SQL Injection

SQL statements, which are entered directly from web to database (interface to interpret SQL) via the web, are not directly passed.

d) OS Command Injection

No shells are allowed to start directly from web.

e) Inadequate Session Management

A session is created after the user successfully logs in, while the user is being authenticated. A session ID is stored as a Cookie while the user is not being authenticated.

3) Response to viruses invading via USB memory

The conceivable use cases for using USB memory are 1) USB direct print, 2)-1 Cloning to USB memory, 2)-2 Cloning from USB memory, 3) Scan to USB, 4) Software update, 5)-1 Backup from SRAM to USB, 5)-2 Restore from USB to SRAM, and 6) Log acquisition; however, there is no risk of infection for the following reasons:

For cases 2)-1, 3) 5)-1 and 6), files are only written from the MFP to USB, and no file is read on the MFP, thus there is no risk of infection.

For cases 2)-2 and 4), encrypted digital signatures are added to software data and cloned data. Since a digital signature is always verified when the file is read, there is no risk of infection.

For 1) and 5)-2, data needs to be written in the MFP and implemented in order to activate a virus-infected file in USB memory inside the MFP. However, since Linux OS is stored in Flash ROM inside the MFP, data is never written in Linux OS, thus, security is ensured. Other programs are stored on the HDD; however, an integrity check is performed to check the program files when power on the MFP. and the event of falsification, a service call error occurs.

1.2.16. Prevention from FAX miss-sending to other destination

1. Function Summary

There is the possibility to leak out confidential information to unexpected address due to miss-dialing or miss-operation in FAX sending. Various functions can be used to prevent this.

2. Current Approach

If prevention of FAX miss-sending is required, changing the setting by requesting a service engineer can prevent the following FAX-miss-sending operations:

- The screen is displayed for confirmation, after inputting the dial before pushing START button.
- The screen is displayed for confirmation, after inputting abbreviated dial or inputting one-touch button. After confirmation, it is possible to send Fax by pushing START button.
- In case of sending Group broadcast transmission, selected group for confirmation is displayed in the screen, and it is possible to send by pushing START button once again.
- Not allowed to operate START button in being on-hook. Moreover, the refusal sounding and the operation are prevented even when pushing the START button.

Once data, which receives in Fax for secret reception, is stored in HDD inside MFP, and then it can be received by entering passwords.

1.2.17. e-BRIDGE Open Platform Security

1. Function Summary

Meta Scan function (Option: GS-1010) and Embedded Web Browser function (Option: GS-1020), which provides Embedded Web Browser and Web Service interface are supported in, e-BRIDGE Open Platform. With using user authentication function, which can be limited to operate MFP panel, the security of these function can be kept. After scanning operation, confidential data to be stored is protected from falsification and leakage by the 3rd party.

2. Current Approach

User Authentication function

In department management or user authentication, neither Embedded Web Browser nor Meta Scan function can be used without authentication. There are two methods to register/manage user information utilized in user authentication:

1) Regarding department management, up to 1,000 departments can be registered and used. Also, up to 10,000 users can be registered in the MFP.
2) It can be coordinated with the user authentication system established in the corporation. Available user authentication systems are the Windows authentication system (Active Directory) that is generally widely used directory services, and LDAP. As for authentication method, in addition to entering an ID and password on the keyboard, a non-contact IC card, HID/Mifare, etc. which provides both convenience and security, can be used as an optional authentication device. This authenticates a user and allows him/her to use the MFP just by holding a HID/Mifare, etc. card onto the card reader connected to the MFP, eliminating a cumbersome password entry on the control panel. Also, as the existing corporate ID card (HID/Mifare, etc) used to enter/leave a room can be used for operating the MFP without making any changes, this method can be introduced at low cost.

Encrypted PDF

When the Meta Scan function is used to select encrypt PDF for a scanned image, the image file is encrypted. By entering the password (user password), the encrypted PDF document can be displayed. An encryption level can be selected from 128-bit RC4 compatible with Acrobat 5.0 and PDF V1.4, 40-bit RC4 compatible with Acrobat 3.0 and PDF V1.1, 128-bit RC4 compatible with Acrobat 6.0 and PDF V1.5, and 128-bit AES compatible with Acrobat 7.0 and PDF V1.6. Operation restrictions can be set for Print, Documents Change, Contents Extraction and Accessibility, respectively. The restriction setting information is protected by password (master password). If the encrypted PDF document is sent to a wrong destination or sniffed, this function prevents users who do know the password from viewing the document. This function also protects distributed PDF documents from unauthorized printing or tampering.

SSL/TLS Support

When the Web Service Scan (Web Services on Device Scan) function is used, communication can be switched to SSL/TLS only in TopAccess. When the Embedded Web Browser function (Option: GS-1020), which provides Embedded Web Browser and Web Service interface, is ready to accept SSL/TLS communication on the external LDAP server, SSL/TLS communication is enabled.

1.2.18. Protection of Confidential Data

1. Function Summary

When replacing or abandoning MFP, some people may be concerned that the person can recreate a document from residual data on the HDD, memory or an e-Filing Box and may be able to steal confidential and private information.

2. Current Approach

After completion of the use of the MFP or at the end of the lease period, a service engineer initializes the HDD according to the customer's instructions. This data overwrite kit also has a function to overwrite meaningless data and completely erase residual data in all HDD areas. A service engineer performs this function according to the customer's instructions. Therefore, the retrieval of residual data on the HDD is completely disabled.

The service engineer can also invalidate data on the HDD. The data on the HDD is instantly erased, enabling the HDD to be reused.

In the case that confidential data remains in the memory of the MFP without a HDD, a service engineer performs a function to clear memory according to the customer's instructions after completion of the use of the MFP or at the end of the lease period. Then, personal data such as telephone numbers set by the customer and data that is not printed out after agency reception can be erased. When the service engineer removes battery, all residual data in the memory can be erased.

For SSD Data, after completion of the use of the MFP or at the end of the lease period, a service engineer initializes SSD according to the customer’s instructions. Also, SSD has a function that meaningless data is overwritten on all area of SSD and the residual data of SSD is all erased. After completion of the use of the MFP or at the end of the lease period, a service engineer can work this, according to the customer’s instruction.

Therefore, it is completely impossible to read out the residual data of SSD.

1.2.19. Protection of Fax received Data

1. Function Summary

Some customers may be concerned about the leakage of confidential information when receiving faxes that are printed during holidays or at night.

2. Current Approach

(1) Fax Secure Receive Function
The Fax Secure Function is used to prevent the leakage of confidential information. The Fax Secure Receive Function is enabled either in administrator or user mode. The Start time (SECURE RECEIVE ON STATE) and end time (SECURE RECEIVE OFF STATE) can be set for days of the week in administrator mode.

SECURE RECEIVE ON STATE:
The Secure Receive Function is enabled and the received data is accumulated in the MFP instead of being automatically printed.

SECURE RECEIVE OFF STATE:
The Secure Receive Function is enabled and the received data is immediately printed.

To print a data received by Fax, which is retained in the MFP during Secure Receive:
- Output(print out) the retained data after Secure Receive is completed.
- Enter the password

To print a data, which is received in SECURE RECEIVE ON STATE:
- Enter the password to output the data received in SECURE RECEIVE ON STATE:
- Click [Print] and select [Secure Receive(Line1)]
- Enter the password to print the data from Line1 or Line2

When data received by Fax is stored in the HDD of the MFP, you can output this data by entering the password. The Fax Secure Function is automatically disabled when the Fax Hold Function is enabled. Even if Secure Receive is scheduled, data is stored in the Fax Hold queue when the Fax Hold Function is enabled.
When data is received in SECURE RECEIVE ON STATE, a message indicating the presence of received data appears at the bottom of the MFP panel. The message remains until all the data is printed.

When data is received in SECURE RECEIVE ON STATE, the data LED also turns on. The LED remains on until all the data is printed. The LED remains on if the MFP goes into sleep mode when received data is present. The LED turns off, however, if the MFP goes into super sleep mode when received data is present.

(2) Fax Hold Function
The Fax Hold Function is used to prevent the leakage of confidential information received by Fax. The Fax Hold Function can only be enabled by a service engineer. If you need to use this function, please contact the service engineer.

When the Fax Hold Function is enabled, data received by Fax is always stored in the Fax Hold queue.
And users initially registered as “Faxope” users, or users assigned as “Fax Operators” can output the data stored in the Fax Hold queue.
To output the data, click [Print] and select [Hold print (Fax)].
The “Fax Operator” role can be assigned to any user using the administrator mode.

When the Fax Hold Function is enabled and data is received by Fax, a message indicating the presence of received data appears at the bottom of the MFP panel and the LED turns on.

1.2.20. e-BRIDGE CloudConnect Security

1. Function Summary

e-BRIDGE CloudConnect securely and reliably collects operation data transmitted from your MFPs.

2. Current Approach

e-BRIDGE CloudConnect uses the same principles used by client PCs accessing secure data over a browser with HTTPS (server authentication and encryption). Data can only be sent from MFPs and access is limited to e-BRIDGE CloudConnect servers with valid authentication certificates. This provides excellent security.

To prevent server spoofing and to make sure data is transmitted to the correct server, e-BRIDGE CloudConnect features server authentication functionality that confirms whether the server to be accessed (e-BRIDGE CloudConnect) is the actual server that was specified. All transmitted and received data is encrypted to preserve its confidentiality and safety, and to protect against stealing, leaking, and tampering.

e-BRIDGE CloudConnect only handles the device operation status information. This includes data concerning charging and maintenance such as information on counter data (the number of sheets used, etc.), device failures, consumables' replacements, and device settings and adjustments. Since e-BRIDGE CloudConnect does not handle actual document data, copy, fax, print and scan data will not be leaked to third parties. On request, a service technician can set e-BRIDGE CloudConnect to permit or deny transmission.

The equipment is operated and managed based on the system's security policy, in accordance with the ISO 27001 international standard for information security management.

2. COMPLIANCE

2.1. Products

ISO/IEC15408 (Information Technology Security Evaluation Criteria) is an international standard for evaluating and certifying functionality and quality of IT products. The functionality and quality of certified IT products have been accepted in many countries participating in the Common Criteria Recognition Arrangement (CCRA).

The Scrambler Board (GP-1010) for the e-STUDIO550/650/810 obtained ISO/IEC15408 EAL2 certification in March 2004, and the Scrambler Board (GP-1031) for the e-STUDIO3511/4511 obtained ISO/IEC15408 EAL2 certification in March 2005. The Data Overwrite Kit (GP-1060) for the e-STUDIO520/600/720/850, e-STUDIO281C/351C/451C, e-STUDIO202L/232/282, and e-STUDIO352/452 obtained ISO/IEC15408 EAL3 in March 2006.

EAL stands for Evaluation Assurance Level, which indicates the levels of assuring the evaluations. Target IT products are evaluated in accordance with the requirements defined by EAL. The higher EAL includes the requirements of the lower EAL. However, EALs represent evaluation strictness, not security strength. EALs are not always corresponding to the security level of the evaluated products. Although the Scrambler Board (GP-1010 and GP-1031) and the Data Overwrite Kit (GP-1060 and GP-1070) obtained EAL2 and EAL3 certification, they are not inferior to higher EALs in security vulnerability.

Model Name	Acquisition	URL
e-STUDIO3511/4511	Certified in March 2005	—
e-STUDIO600/720/850	Certified in March 2006	—
e-STUDIO281C/351C/451C	Certified in March 2006	—
e-STUDIO232/282	Certified in March 2006	—
e-STUDIO352/452	Certified in March 2006	—
e-STUDIO2500C/3500C/3510C	Certified in June 2006	—
e-STUDIO163/165/205	No scheduled to be certified	—
e-STUDIO166/167/207	No scheduled to be certified	—
e-STUDIO232/282	Certified in August 2008	—
e-STUDIO352/452	Certified in August 2008	—
e-STUDIO600/720/850	Certified in August 2008	—
e-STUDIO2330C/2820C/2830C/ 3520C/4520C	Certified in December 2008	—
e-STUDIO5520C/6520C/6530C	Certified in December 2008	—
e-STUDIO255/355/455	Certified in June 2009	—
e-STUDIO655/755/855	Certified in June 2009	—

e-STUDIO2040C/2540C/3040C/3540C/4540C	Certified in October 2011	http://www.ipa.go.jp/security/jisec/certified_products/c0328/c0328_it0296.html
e-STUDIO5540C/6540C/6550C	Certified in October 2011	http://www.ipa.go.jp/security/jisec/certified_products/c0327/c0327_it0297.html
e-STUDIO206L/256/306/356/456/506	Certified in May 2012	http://www.ipa.go.jp/security/jisec/certified_products/c0348/c0348_it1388.html
e-STUDIO556/656/756/856	Certified in May 2012	http://www.ipa.go.jp/security/jisec/certified_products/c0349/c0349_it1389.html
e-STUDIO2050C/2550C	Certified in October 2012	http://www.ipa.go.jp/security/jisec/certified_products/c0376/c0376_it2409.html
e-STUDIO2555C/3055C/3555C/4555C/5055C	Certified in April 2013	http://www.ipa.go.jp/security/jisec/certified_products/c0388/c0388_it2432.html
e-STUDIO306LP	Certified in November 2013	http://www.ipa.go.jp/security/jisec/certified_products/c0412/c0412_it3465.html
e-STUDIO5560C/6560C/6570C	Certified in November 2015	http://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0491/c0491_it4484.html
e-STUDIO207L/257/307/357/457/507	Certified in November 2015	http://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0489/c0489_it4482.html
e-STUDIO557/657/757/857	Certified in November 2015	http://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0490/c0490_it4483.html
e-STUDIO2000AC/2500AC	Certified in September 2016	http://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0522/c0522_it5581.html
e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC	Certified in September 2016	http://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0523/c0523_it5582.html
e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A	Certified in September 2016	http://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0524/c0524_it5583.html
e-STUDIO5506AC/6506AC/7506AC	Certified in November 2016	http://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0528/c0528_it5584.html
e-STUDIO5508A/6508A/7508A/8508A	Certified in November 2016	http://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0529/c0529_it5585.html

e-STUDIO3508LP/4508LP/5008LP	Certified in July 2017	http://www.ipa.go.jp/security/jisec/jisec_e/certified_products/c0566/c0566_it6624.html

2.2. Regulatory Requirements

With the passing of numerous government regulatory acts, it is imperative that hardware and software solutions address the security issue. The solutions provided by Toshiba specifically focus on:

- **HIPAA** – The Health Insurance Portability and Accountability Act designed to ensure that patient information is treated with the highest level of confidentiality both within the healthcare organization and outside of the organization. Toshiba security solutions offer various features that address the privacy and security of protected patient information. Secure device access, private printing capabilities, and an audit trail prevent improper device usage and only allow authorized users to receive the confidential data or documents.
- **GLB Act** – The Gramm-Leach-Bliley Act relates directly to financial institutions, ensuring that consumer's are aware of how their personal financial information is being used and shared. The Financial Privacy Rule and Safeguards Rule govern the disclosure of private financial information and require all financial institutions to design and maintain systems to support the protection of customer information.
- **FERPA** – The Family Education Rights and Privacy Act is a federal law that protects the privacy of student education records. This requires a heightened level of security for educational institutions complying with the U.S. Department of Education. Password printing, controlled device access, data encryption and/or deletion ensure that sensitive information is not accessible on the multifunction device.

- The **Sarbanes-Oxley Act** (SOX) recently introduced stringent rules with the objective to change financial practices and corporate governance regulations. Following high profile corporate scandals, such as Enron, this was passed to protect investors by improving the accuracy of corporate financial disclosures made in relation to the securities laws. Data security safeguards focus on restricting access to information, the tracking of data, and protection of data integrity.

- CCEVS - Common Criteria Evaluation and Validation Scheme established by the National Information Assurance Partnership (NIAP) evaluates information technology products for conformance to certain security standards. The **Common Criteria** program recognizes and validates security solutions based upon an internationally accepted methodology. Toshiba products currently comply with the Common Criteria and are EAL Certified conforming to ISO/IEC15408 (Information Technology Security Evaluation Criteria).

DoD – The Department of Defense, directly under the President of the United States of America, formulates national security and defense policies. The Department of Defense Manual outlines rigid policies and standards in the interest of protecting the security of the United States. Toshiba's Disk Overwrite solution complies with the DoD standard of clearing and sanitizing a hard disk drive containing classified information.

Act for Protection of Computer-Processed Personal Data Held by Administrative Organs

As the information society advances, personal information is becoming an increasingly important asset. In the meantime, cases where personal information is illegally collected and used for unexpected purposes without notifying relevant individuals are increasing and the society is becoming more concerned about the handling of personal information. Under such circumstances, the Act for Protection of Computer-Processed Personal Data Held by Administrative Organs went into effect in full-scale in April 2005.

Once a large amount of personal information leaks, the company will not only lose credibility but also fall into a dangerous situation that may cause serious damage endangering company's existence. It is a social responsibility for companies to establish a good relationship of trust with customers, make an effective use of personal information, and protect it as well.

The Act for Protection of Computer-Processed Personal Data Held by Administrative Organs, prescribes such responsibility for identifying personal information the organization is handling, clearly expressing the purpose of use to each individual that possess the personal information, and managing the information to prevent it from being used for any purposes other than specified.

Toshiba TEC Corporation provides products equipped with a wide variety of the aforementioned security features, to allow its customers to avoid information leak. Toshiba TEC Corporation will enhance the partnership with customers and move forward with implementing safer security measures.

Toshiba TEC Corporation recognized the importance of personal data protection at an early stage and established the Privacy Policy and the Personal Data Protection Guidelines as in-house regulations, in February 2001.

The personal data protection system has been improved. The Privacy Policy was amended and published on the web site in August 2004. The Personal Data Protection Guidelines were significantly revised in accordance with regulatory requirements in November 2004 and re-established as the Personal Data Protection Program (PDPP).

The Toshiba TEC Corporation's Privacy Policy established on February 7, 2001 and amended on August 27, 2004, is mentioned on the following pages.

Toshiba TEC's Privacy Policy

Amended on August 27, 2004

Toshiba TEC Corporation ("Toshiba TEC") will observe the following privacy policy in its business activities, while recognizing the value and usefulness of personal data.

1. Compliance with laws and regulations

   Toshiba TEC will comply with all laws and regulations related to personal data.

2. Specification of use

   Whenever Toshiba TEC asks for personal information, it will specify in advance the purposes for which such information will be used, and will restrict the use to those purposes. If Toshiba TEC should ever need to use personal data for purposes other than those specified, it shall inform the individuals concerned of the additional purposes. Any individual may refuse to have personal data used for such additional purposes. Individuals who do not wish to provide Toshiba TEC with personal data can withhold consent, though doing so may prevent access to certain services that Toshiba TEC provides.

3. Non-disclosure to third parties

   In principle, Toshiba TEC does not disclose or provide personal data to third parties, except in the following circumstances.

   1) When express consent to do so is received from the person concerned.
   2) When an inquiry concerning a product or service can be more appropriately handled by a Toshiba TEC subsidiary or affiliate which is responsible for that product or service.
   3) When Toshiba TEC consigns such activities as promotional campaigns or competitions to other entities, in which case personal data is covered by the terms of a non-disclosure agreement.
   4) When it is necessary to complete the settlement of payment for products ordered or services provided (e.g. providing information to financial institutions to facilitate credit card transactions, etc.)
   5) When a judicial order or the like obliges Toshiba TEC to disclose personal data.
   6) When business is transferred to another entity by way of a merger, corporate separation or otherwise.

4. Inquiries

   Individuals who wish to confirm their personal data should contact the section responsible for the services where they input the information. Toshiba TEC will provide the personal data that it has when it has confirmed that the individual making the inquiry is the person concerned. This restriction applies to prevent leakage of personal data to third parties. When personal data contains errors or needs to be updated, Toshiba TEC will make the required changes, when it has confirmed that the individual making the request is the person concerned. This restriction applies to prevent improper alteration of personal data by third parties.

5. Security measures

   Toshiba TEC implements strict security measures to ensure that personal data is not improperly accessed, leaked, lost, destroyed or dishonestly altered.

6. Implementation of the Privacy Policy

   Toshiba TEC will diligently implement the Privacy Policy and will continuously review it for improvement.

Takayuki Ikeda

President and Chief Executive Officer