TOSHIBA
Leading Innovation >>>

- Securing Devices
- Controlling Access
- Protecting Documents
- Safeguarding All Valuable Data

secureMFP™

Keeping your business your business.

Your business may be at risk. Toshiba can help.

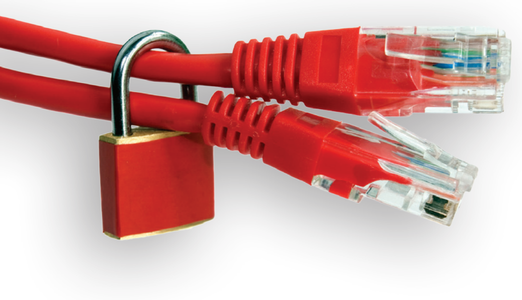
Security is a growing concern for companies of all sizes. With Toshiba SecureMFP,™ we employ innovative methods of protecting valuable data in order to help businesses of all sizes meet the increasing security challenges.

Protect Your Data and Your Business

The Association of Certified Fraud Examiners found that companies in the United States lose more than $600 billion a year due to fraud, and document fraud is a large part of this statistic. Now that MFPs (Multifunction Products) and laser printers are able to store data, they've become an integral part of business networks, and a critical point of vulnerability. They retain latent document images and contact information, leaving sensitive information and mission-critical data at risk. These threats to security can come from anyone, anywhere.

The 2013 Data Breach Investigation Report found that 92% of security breaches resulted from external sources and 14% were traced to insiders. Reports from a variety of resources have come to these same conclusions: data theft is common, it happens regularly, and everyone is aware that it's a serious problem. That's why we deliver serious security solutions. In addition to protecting against security breaches and possible litigation, we assist in keeping businesses compliant with ever-increasing government regulations such as HIPAA, FERPA, Sarbanes-Oxley, and eDiscovery, to name a few.

- **Over $600 billion lost each year to fraud**
- **1 in 5 security breaches come from inside**
- **Left unsecured, an MFP can pose one of the greatest threats to your organization**
- **The average total cost per company that report a data breach in 2012 was more than $5.4 million**



That networked MFP in the corner of your office just might be the most significant entry point for hackers to hijack sensitive data from your business.

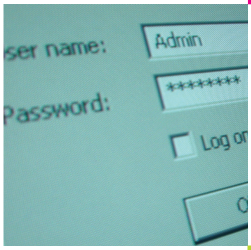
secureMFP™

Device Security

In order to protect the confidentiality and integrity of your data, we continually develop comprehensive security measures for Toshiba devices. Most of our MFPs come standard with **Self-Encrypting Drive (SED)** technology that allows sensitive user data to be securely erased when a system is powered-down or when a SED Hard Disk Drive (HDD) is removed from the system and encryption. In addition, the disk is automatically cleared immediately after the device is done using information after every job, preventing the data from being recovered by unauthorized users. This Toshiba-exclusive design utilizes the 256 Advanced Encryption Standard (AES) and is FIPS 140-2 (Federal Information Processing Standards) certified, while the data overwrite kit meets Department of Defense requirements.

Because MFPs and network printers function as complex network devices, we have developed several solutions that specifically address network security. **IPv6** ensures IP security with a larger IP address range, protection from scanning and attacks, and support for authentication and confidentiality as part of our optional IPsec. **Secure Sockets Layer (SSL)** employs encryption technology to protect all data traveling to and from the MFP, while **IP Filtering** acts like a firewall to protect your internal network from intruders. Also, **SMB Signing** adds a digital signature to verify that data is received from authenticated sources and ensures the integrity of all communications.

Access Security



Toshiba has developed simple yet highly effective methods of establishing access security without inconveniencing users. **Network Authentication** allows administrators to control access at the device in the same way it's controlled from the desktop. **Department Codes** provide valuable data tracking and usage information, giving authorized users full functionality at the device. **Usage Limitations** enable administrators to set limits for copy and print jobs, as well as track and control costs. **Strong Passwords** utilizes a ten-digit alphanumeric administrative password for added protection along with a log-on attempt limitation. To streamline the user login process, our **SmartCard Authentication** requires the simple swipe of a card while allowing limited user access to specific features and functions.

- **Secures Print Output**
- **Protects Data**
- **Creates Secure PDF**
- **Controls Access**
- **Encrypt Scanned Documents**

Control access to your MFP with Network Authentication.

Security where it counts, because it counts everywhere.

Toshiba takes the security of your documents very seriously. And we are ready to help protect your critical data with our suite of Digital Rights Management (DRM) Solutions from Fasoo. Fasoo is a world leader in Enterprise DRM with more than a decade of experience in the industry.

Document Security

Fasoo's DRM applications will help your company provide even greater protection against unauthorized access to sensitive financial, technical and personal information. You can easily control access to Microsoft Office Documents, PDFs, engineering drawings, images and other common file formats. These threats come from both inside and outside of your organization, and this technology helps you to better address these risks.

Fasoo DRM Enables You to:

- Prevent unintended information disclosure or exposure
- Ensure a secure information sharing environment
- Better manage workflows and simplify secure collaboration
- Deploy Secure Print Control & Policy including digital watermark

Fasoo DRM is the best core security infrastructure for organizations struggling to reduce data loss and improve work efficiency.

Reliable Protection:

Constantly protects files, including shared files for legitimate uses throughout the document lifecycle.

- Data at Rest
- Data in Transit
- Data in Use

Protect Sensitive Documents:

- Auto Encryption based on User/Group (LDAP)
- Context based Encryption (PII, PHI)

Cloud and Mobile Security Strategy:

- Protect Mobile device
- Manage Mobile security and control
- Policy enforcement in Cloud environment

Dynamic Permission Controls:

Controls file access privileges of users, groups and/or environments including external users.

- Who & Where (user, group, device and network address)
- How (view, edit, print, copy/paste, screen capture and decrypt)
- When (expiration date, validity period and how many times)

Extended Features of Fasoo DRM

- **Revokes documents after delivery with a dynamic permission control.**
- **Prevents unauthorized use of screen capture tools, remote desktop software and virtual machines.**
- **Supports native applications and file formats that are transparent to users.**

Fasoo

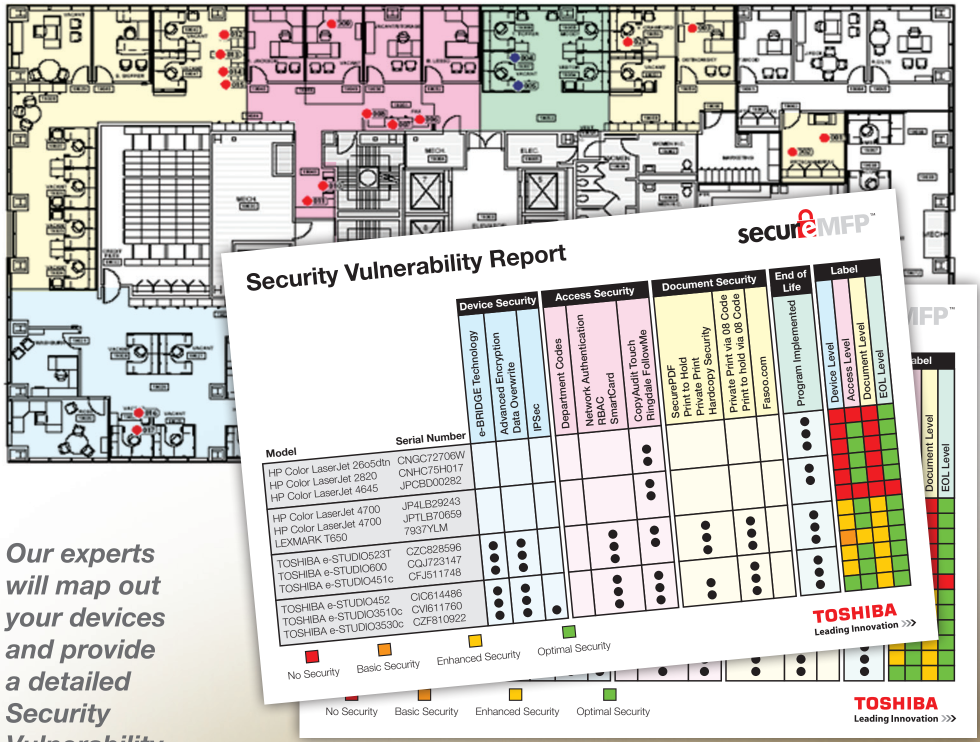
Audit Trail:

Tracks activities of users, files changes in configuration.

- Who (user and group)
- What (document name and path)
- How (view, edit, print and decrypt)
- Where (IP address)
- When (time log)

secureMFP™

TOSHIBA
Leading Innovation >>>



Security Vulnerability Report

secureMFP™

		Device Security			Access Security			Document Security			End of Life	Label			
Model	Serial Number	e-BRIDGE Technology	Advanced Encryption Data Overwrite	IPSec	Department Codes	Network Authentication RBAC SmartCard	CopyAudit Touch Ringdale FollowMe	SecurePDF Print to Hold Private Print Hardcopy Security	Private Print via 08 Code Print to hold via 08 Code	Fasoo.com	Program Implemented	Device Level	Access Level	Document Level	EOL Level
HP Color LaserJet 26o5dtn HP Color LaserJet 2820 HP Color LaserJet 4645	CNGC72706W CNHC75H017 JPCBD00282						● ●				● ● ●	🟥 🟥 🟥	🟥 🟩 🟩	🟥 🟥 🟥	🟩 🟩 🟩
HP Color LaserJet 4700 HP Color LaserJet 4700 LEXMARK T650	JP4LB29243 JPTLB70659 7937YLM						● ●				● ●	🟥 🟥 🟥	🟩 🟩 🟥	🟥 🟥 🟥	🟩 🟩 🟥
TOSHIBA e-STUDIO523T TOSHIBA e-STUDIO600 TOSHIBA e-STUDIO451c	CZC828596 CQJ723147 CFJ511748	● ● ●	● ● ●			● ● ●	● ●	● ● ●	● ● ●		● ● ●	🟨 🟨 🟧	🟩 🟩 🟨	🟨 🟨 🟨	🟩 🟩 🟩
TOSHIBA e-STUDIO452 TOSHIBA e-STUDIO3510c TOSHIBA e-STUDIO3530c	CIC614486 CVI611760 CZF810922	● ● ●	● ● ●	●		● ● ●	● ● ●	● ●	● ● ●		● ● ●	🟨 🟨 🟩	🟩 🟩 🟩	🟨 🟨 🟨	🟩 🟩 🟩

🟥 No Security 🟧 Basic Security 🟨 Enhanced Security 🟩 Optimal Security

TOSHIBA
Leading Innovation >>>

Encompass Security Assessment

Toshiba utilizes innovative security technologies and expert personnel who are trained and certified as part of our Encompass Security Vulnerability Assessment Program. Our Professional Services Consultants will:

- Assess device, technology, document and process
- Assess all points of vulnerability including brands and devices that may not be manufactured by Toshiba
- Provide a recommendations report to mitigate a security concern
- Recommend Implementation Strategy to fill in a gap to remedy risk of losing confidential information

Our Encompass Security Assessment includes four areas of focus:

- Device Security
- Access Security
- Document Security
- End of Life/Disposal Security

Our experts will map out your devices and provide a detailed Security Vulnerability Report.

Secure your data, before it leaves the building.

Toshiba has an extensive End of Life Security Policy to ensure all of your critical data is removed from the copier hard drive before it leaves your organization. Toshiba devices, as well as many other brands, can be scrubbed to remove any and all information that may still be stored on the hard disk drive.

MFP End of Life Security Policies

At the end of your lease, you can choose which level of security suits the needs of your organization.

BASIC SECURITY

Basic Security includes removing the uncleansed hard disk drive (HDD) and returning it. You are then responsible for disposing of the HDD. If your MFP has been financed, the lessor requires that the MFP is returned in good operating condition. In this case, a new HDD is then installed and reloaded with system firmware so that the MFP will be operational.

Security Procedure:

- Remove and return uncleansed HDD to customer
- Install new HDD
- NVRAM and Fax Data Scrub

ENHANCED SECURITY

Enhanced Security includes overwriting all of the data on your existing Toshiba MFP, including NVRAM and Fax data. If your MFP has been financed, the lessor requires that the MFP is returned in good operating condition. In this case, reloading the system firmware is required so that the MFP will be operational. This level ensures that data is irretrievable and that the HDD is restored to functional status.

Security Procedure:

- HDD Data Scrub
- NVRAM and Fax Data Scrub
- Reload System Firmware

OPTIMAL SECURITY

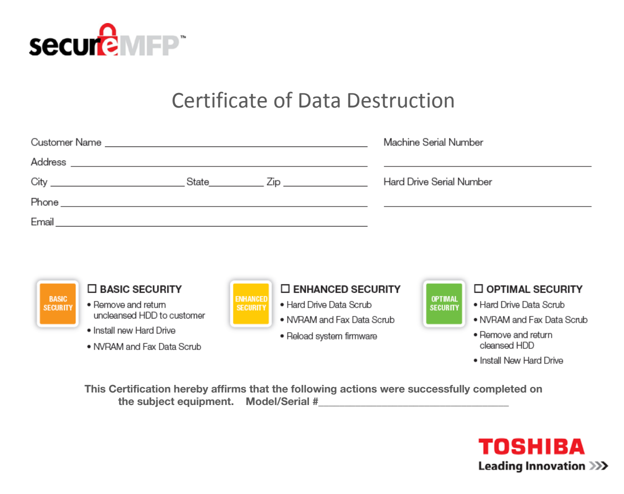
In addition to the procedures included in the Enhanced End-of-Life Security Scrub, Toshiba will provide you with the actual MFP Hard Drive. You are then responsible for disposing of the cleansed HDD. We will install a new functional HDD in the device to restore it to full functionality.

Security Procedure:

- HDD Data Scrub
- NVRAM and Fax Data Scrub
- Remove and return cleansed HDD to customer
- Install new HDD

secureMFP™

TOSHIBA
Leading Innovation >>>



secureMFP™

Certificate of Data Destruction

Customer Name ______________________________ Machine Serial Number

Address ______________________________ ______________________________

City ______________ State________ Zip ____________ Hard Drive Serial Number

Phone ______________________________ ______________________________

Email ______________________________

BASIC SECURITY

□ BASIC SECURITY
- Remove and return uncleansed HDD to customer
- Install new Hard Drive
- NVRAM and Fax Data Scrub

ENHANCED SECURITY

□ ENHANCED SECURITY
- Hard Drive Data Scrub
- NVRAM and Fax Data Scrub
- Reload system firmware

OPTIMAL SECURITY

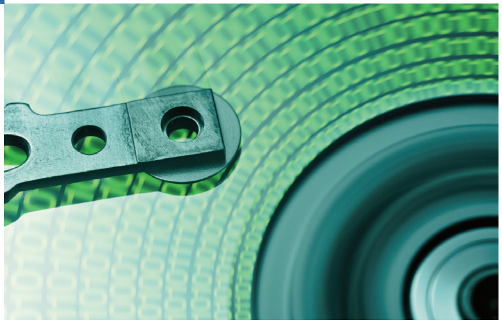
□ OPTIMAL SECURITY
- Hard Drive Data Scrub
- NVRAM and Fax Data Scrub
- Remove and return cleansed HDD
- Install New Hard Drive

This Certification hereby affirms that the following actions were successfully completed on the subject equipment. Model/Serial #______________________________

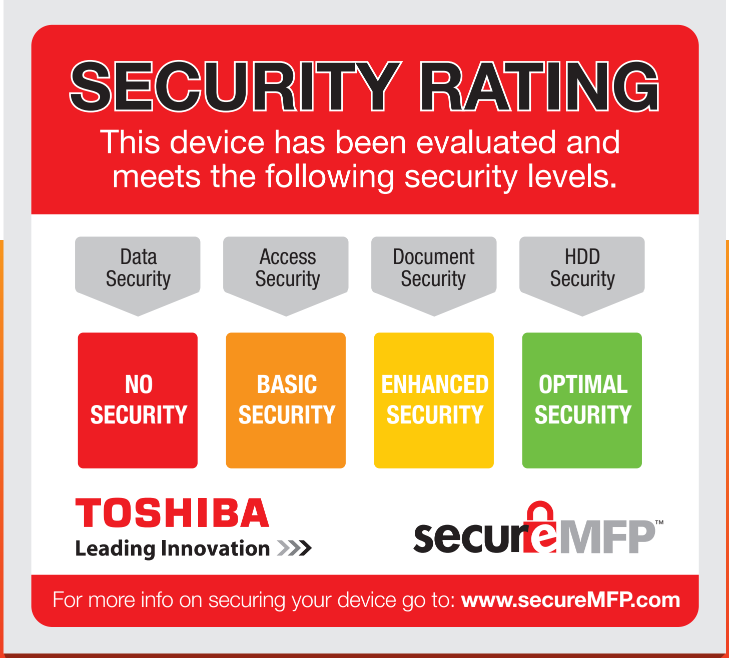
TOSHIBA
Leading Innovation >>>

Certificate of Data Destruction

We will provide you with a Certificate of Data Destruction for all devices that have reached End of Life within your organization.



Remove critical data from your hard disk drive before disposing of your MFP.



SECURITY RATING

This device has been evaluated and meets the following security levels.

Data Security	Access Security	Document Security	HDD Security
NO SECURITY	BASIC SECURITY	ENHANCED SECURITY	OPTIMAL SECURITY

TOSHIBA
Leading Innovation >>>

secureMFP™

For more info on securing your device go to: **www.secureMFP.com**

Protect and Defend

With SecureMFP, each device is assessed and labeled to indicate the level of security. The following four areas of security are identified:

- Device Security
- Access Security
- Document Security
- End of Life/Disposal Security

Toshiba can help you achieve a uniform level of security across your network in order to protect valuable data and intellectual property. Allow one of our Professional Services Consultants to show you how we can best provide the level of security your company requires while reducing revenue losses and ensuring that regulatory requirements are met.

For more info visit **www.securemfp.com**

secureMFP™

TOSHIBA
Leading Innovation >>>

Toshiba's Security Toolkit - Standard with all Toshiba e-STUDIO Devices.

Device

- SSL
- IPv6
- IP Filtering
- SMB Signing
- IPsec*
- Data Overwrite
- Advanced Encryption

Access

- Email Authentication
- Network Authentication
- Role Based Access
- Usage Limitations
- SmartCard Authentication*
- Strong Passwords
- Department Codes

Document

- SecurePDF
- Private Print
- HardCopy Security
- Job Log
- Encryption*
- Digital Watermark*

*Optional security solutions

Certifications & Standards

DoD – The Department of Defense

The U.S. Department of Defense manual outlines rigid policies and standards in the interest of protecting the security of the United States. Toshiba meets these policies with Disk Overwrite solutions that clear and sanitize hard disk drives that may contain classified information.

CCEVS – Common Criteria Evaluation and Validation Scheme

The CCEVS program recognizes and validates security solutions based upon an internationally accepted methodology. Toshiba products comply with the Common Criteria Evaluated Assurance Level 3 (EAL 3), and conform to ISO/IEC15408 (Information Technology Security Evaluation Criteria) and meets IEEE 2600.1 criteria.

FIPS – Federal Information Processing Standard

FIPS (Federal Information Processing Standard) 140-2 is a US government standard that describes the encryption and related security requirements that IT products should meet. The standard provides four increasing, qualitative levels of security. The standard ensures that a product uses robust security practices, such as strong encryption algorithms and methods. It also specifies how modules or components must be designed to interact securely with other systems. Toshiba HDD is FIPS 140-2 Level 2 certified.

CAC/PIV - Common Access Card/ Personal Identity Verification

For U.S. government agencies, Toshiba meets Homeland Security Presidential Directive (HSPD-12) by facilitating Common Access Card (CAC/PIV) multi-factor authentication required by the U.S. Department of Defense (DoD) for access to network-based devices.

Regulatory Compliance

HIPAA – The Health Insurance Portability and Accountability Act

Toshiba security solutions offer advanced features that address the privacy and security of protected patient information, including secure device access, private printing capabilities, an audit trail, and features that allow only authorized users to receive confidential data or documents.

GLB – The Gramm-Leach-Bliley Act

The Financial Privacy Rule and the Safeguards Rule mandated through the Gramm-Leach-Bliley Act pertain to the disclosure of private financial information. The rules require all financial institutions to design and maintain systems to support the protection of customer information. Toshiba products support this directive.

FERPA – The Family Education Rights and Privacy Act

FERPA requires a heightened level of security for educational institutions in order to comply with the U.S. Department of Education. Password-restricted printing, controlled device access, and data encryption and/or deletion ensure that sensitive information is protected on Toshiba multifunction devices.

SOX – The Sarbanes-Oxley Act

Corporate governance regulations such as the Sarbanes-Oxley Act are enforced on Toshiba MFP devices through data security safeguards focused on restricting access to information, tracking data, and protecting data integrity.

Corporate Office 9740 Irvine Blvd., Irvine, CA 92618
Tel: 949-462-6000

East Coast 959 Route 46 East, 5th Floor, Parsippany, NJ 07054
Tel: 973-316-2700

Midwest 8770 W. Bryn Mawr Ave., Suite 700, Chicago, IL 60631
Tel: 773-380-6000

South 2037 Bakers Mill Rd., Dacula, GA 30019
Tel: 678-546-9385

West Coast 9740 Irvine Blvd., Irvine, CA 92618
Tel: 949-462-6000

Web Site www.business.toshiba.com