secureMFP

Complete document security

Protect your valuable data at every stage of your workflow

TOSHIBA
Leading Innovation

Toshiba Security Solutions

Without a doubt, security is one of the most important issues facing today's business environment. Significant resources are devoted to creating secure and compliant corporate network infrastructures, and the same diligence must be applied to other aspects of the enterprise. Your multifunction print, copy, scan, and fax devices are no exception — data communication within the corporate network must be securely transmitted and received.

DATA SECURITY SOLUTIONS FOR TOSHIBA MFPS

Whenever pages are printed, copied, scanned, or faxed, your digital Multifunction Peripheral (MFP) device retains data in its internal memory. Without proper security measures in place, this data can be retrieved by unauthorized persons. Additionally, unrestricted access to the device can lead to security breaches.

Toshiba recognizes the importance of maintaining a stringent security initiative, and recent federal regulations have only re-emphasized the need for a secure network environment. With Toshiba MFP products, the same level of data integrity and accountability is enforced regardless of whether data is sent from inside or outside your network firewall.

Whether you deal with personal or financial information or health records or simply need to protect sensitive corporate data, your MFPs need to provide heightened security while minimizing risks. In order to avoid any potential security compromises, Toshiba MFPs are designed to address security issues in three distinct ways:

- Controlling access to the device and data
- Providing data tracking and accountability
- Securing communication

These safeguards ensure that stored or transmitted data is not compromised from within the corporation. They are specifically designed to prevent unauthorized access to multifunction products that could put your business at risk.

Built with security in r

Department Codes

These private, preset codes give authorized users full functionality at the device, allowing them to copy, print, fax, and scan. In addition to controlling access, Department Codes provide valuable data tracking and usage information, allowing network administrators to easily track and view the volume and type of jobs being produced by each department or user.

Network Authentication

Ideal for larger-scale installations with numerous users, Network Authentication allows administrators to control access at the device in the same manner that they control network access from the desktop. Users are required to input their network user name and password to gain access to the control panel. Network Authentication can also be used in conjunction with Role-Based Access Control (RBAC), which allows administrators to specify which MFP functions are available to each individual.

SecurePDF

SecurePDF provides control and protection for scanned documents sent to e-mail and network folders. With SecurePDF, users can assign a password to a scanned document that controls access to viewing, printing, editing, and copying its content. Up to 128-bit encryption can be applied to ensure it is stored safely.

Usage Limitations

Limits can be set for copy and print jobs, including black/white and color output limitations. Usage limitations allow the administrator to control and track output at the device. They also add an additional level of security for controlling access to the device, and provide enhanced visibility by helping track and control costs associated with the device's use.

Private Print

This security feature offers complete control of print output by requiring users to input a password before initiating a print job. Private Print is ideal when printing confidential information because it prevents other people from accidentally or intentionally picking up the wrong print job. Toshiba has made this process even more flexible by giving users the option to print private documents one at a time, or to print multiple private documents and retrieve them all at once, with a single trip to the MFP.

Strong Passwords

Password hacking programs can crack a weak password instantaneously. Toshiba employs a ten-digit alphanumeric administrative password and a log-on limitation of up to three attempts. This process helps foil attempts to crack the administrative password by making it more difficult to ascertain, and by disabling log-on privileges after three failed attempts.

Job Log

The Toshiba Job Log feature makes it easy to track data and documents. Information about each completed job is stored within the e-STUDIO Job Log. Print, fax, and scan jobs are tracked with detailed information including the user name, date, time, number of pages, type of paper, and type of job.

E-mail Authentication

When conducting business via the Internet or e-mail, authentication is critical because it ensures that you are corresponding with your intended recipient. Toshiba's e-mail authentication technology allows organizations to manage the e-mails being sent from each multifunction device.

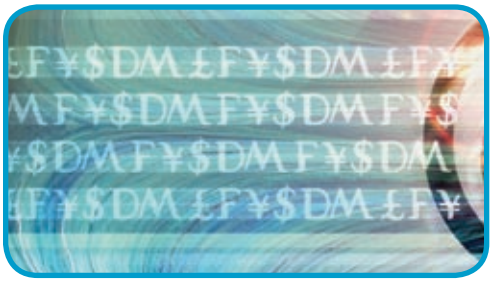
mind, to keep the flow of data safe

Toshiba controls access to multifunction devices through a number of different methods. Corporations may limit access to the device and data through the use of department codes, network authentication, private printing, usage limitations, and administrative password enhancements.

NETWORK SECURITY FEATURES BUILT RIGHT IN TO EVERY E-STUDIO DEVICE

IPv6

IPv6—the latest version of IP—is commonly referred to as the next-generation Internet Protocol. IPv6 introduces several new features that address IP security needs, such as a larger IP address range, protection from scanning and attacks, and built-in support for authentication and confidentiality. Toshiba supports IPv6 as part of our ongoing commitment to meeting your current and future network needs.



Secure Sockets Layer (SSL)

Secure Sockets Layer is a cryptographic protocol widely used on the Internet to provide secure communications for transfer of personal information. MFP devices employ this common encryption technology to protect all data traveling to and from the MFP. Print jobs sent via SSL are encrypted through symmetric cryptography, ensuring that the print data is secure and will not be used for any purpose other than print output.

IP Filtering

IP Filtering acts like a firewall to protect your internal network from intruders. This filtering process lets you control which IP traffic is allowed into and out from your network, by allowing or denying data transfer from specific network addresses. MFP devices utilize this mechanism as a means of controlling which computers have access to its network functions.

SMB Signing

SMB signing adds a digital signature to data transferred between the MFP and the server during network authentication. This signature verifies that the identity of the server matches the credentials expected by the MFP and vice versa. By verifying that data is received from authenticated sources, these signatures ensure the integrity of all communications.

SecureMFP Solutions

Toshiba's team of document security professionals analyzes your company's document and data security workflow and provides security hardware and service options to address your needs. Our solutions ensure that your company stays in compliance with all federally-mandated security directives. SecureMFP solutions are organized into modules that allow you to choose the security level that's right for your business.

SECURITY LEVEL 1

- Provides information security by protecting confidential data and eliminating the threat of data being compromised.
- 128-bit AES and 3DES encryption of all stored data.
- Ensures data is overwritten to prevent any storage of sensitive information on the device.
- Exceeds Department of Defense data scrubbing standards.

Data Overwrite Kit

Each time your MFP processes a copy, print, fax, or scan job, document data is written to its internal hard drive. If your hard drive is compromised or stolen, your sensitive data could be accessed by unauthorized persons. The Toshiba Data Overwrite Kit eliminates this threat by ensuring that all files written to your MFP's internal hard drive are completely erased after each and every copy, fax, scan, or print job. The erased files cannot be recovered, even if the hard disk is removed and installed in a desktop computer.

Scrambler Board

Data Encryption is the most effective way to achieve data security. When your MFP hard drive is protected, your data is secure. The Toshiba Scrambler Board uses 128-bit encryption to protect your data in the event your MFP's hard drive is compromised.

SECURITY LEVEL 2

Includes all of the features of Level 1, plus:

- Restricts and locks down access to the device.
- Access control invoked via contactless card identification.
- Individual user's rights can be restricted to specific functionality and features.
- Guarantees that unauthorized users do not have access to the device.

SmartCard Authentication

Toshiba's SmartCard Authentication offers extensive security features that are designed to put an end to unauthorized operation, while reducing costs and downtime. A time-saving, single point of entry streamlines the user login process by requiring a simple card swipe instead of typing a user name and password on the keypad. You control who has authorization to use each device, which features they are allowed to use, as well as the ability to limit color usage and the number of copies, scans, and faxes that can be produced.

SECURITY LEVEL 3

Includes all of the features of Levels 1 and 2, plus:

- Restricts and locks down access to the device.
- Access control invoked via contactless card identification.
- Individual user's rights can be restricted to specific functionality and features.
- Guarantees that unauthorized users do not have access to the device.

FollowMe Printing

FollowMe enhances document security by holding print jobs in a centralized queue until the user logs on to the MFP for authentication. Users can retrieve their printed documents from any FollowMe-enabled MFP on the network. Since the document originator is required to be physically present at the MFP before any pages are printed, there's no need to worry about unauthorized persons retrieving sensitive documents from the MFP. As an added benefit, FollowMe reduces waste that occurs when individuals send documents to a printer, then fail to collect them.

SECURITY ADD-ONS AND OPTIONS

- Toshiba also provides additional security solutions to enhance Level 1, 2, or 3.

e-BRIDGE Re-Search

A powerful e-Discovery software tool to manage your electronic data and perform lightning-fast searches.

Data Deletion

Completely eliminate residual data on your MFP when it is retired or replaced.

secureMFP

Are you in compliance?

DOCUMENT SECURITY

To protect your valuable data and intellectual property, a uniform level of security must be applied consistently across your entire network. That goes for your desktop, your multifunction devices, and any other networked peripherals. With so many regulatory and compliance measures to respond to, Toshiba has looked to the federal government requirements, among others, as guidelines. Government regulations establish strict criteria for security adherence. While not all organizations are held to these regulations, Toshiba MFP security features address the security requirements of many government directives.

TOSHIBA SECURITY SOLUTIONS MEET OR EXCEED:

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.

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, and conform to ISO/IEC15408 (Information Technology Security Evaluation Criteria).

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.

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's Disk Overwrite solution clears and sanitizes hard disk drives that may contain classified information.

eDiscovery – New Federal Rules of Civil Procedure

A federal eDiscovery mandate went into effect December 1, 2006, that governs when and how information is collected, preserved, and produced in connection with legal discoveries for every case pending in any U.S. Federal Court. In summary, the new eDiscovery rules do not require companies to keep all content forever, though they do affect the following areas:

- Discovery – ESI or "electronically stored information" is now definitively subject to legal discovery.
- Transparency – Companies are now required to make their IT departments available to lawyers.
- Preservation – Whenever a company is placed on notice of a new case, the company must identify the information that is potentially relevant to that case and preserve it for subsequent production to the other side in the case.

Corporate Office: 2 Musick, Irvine, CA 92618-1631 / Tel: 949/462-6000 / 800-GO-TOSHIBA
Web Site: www.copiers.toshiba.com