

Security is a growing concern, even for small and medium sized businesses. With Toshiba SecureMFP, we employ innovative methods of protecting valuable data in order to help businesses of all sizes meet increasing security challenges.

Security as a business strategy encompasses several areas each of which requires detailed consideration. Toshiba is cognizant of the challenges of each phase and offers technological solutions to assist at each stage.

DEVICE SECURITY

In order to protect the confidentiality and integrity of your data, we continually develop comprehensive security measures for Toshiba devices. Our Advanced Encryption functionality provides on-the-fly encryption and decryption of data written to the device's hard drive. The Data Overwrite Kit ensures that all data is erased after every fax, copy, scan and print job in order to prevent the latent storage of valuable data on the device. 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 & MAC 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.

DOCUMENT SECURITY

With Digital Rights Management (DRM), security policies remain with each document as it travels inside and outside of your organization. To preserve the integrity and security of printed information, Private Print (locked print) prevents the wrong person from picking up the wrong print job and gives the user the option of printing private documents individually or multiple documents at one time.

Secure server printing holds print jobs in a central queue until the user logs on to any Secure server printing enabled MFP, ensuring that the correct user is physically present before the document is printed.

SecurePDF protects scanned documents, enabling users to assign a password in order to restrict viewing, printing, editing and copying of the scanned information. Up to 128-bit encryption can be used to keep the information safely stored.

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.

Authenticated users allows the control of MFP feature access based on an Active Directory profile. Toshiba's Role Based Access Control can filter access to individual features at the MFP based on the user.

END-OF-LIFE DATA SCRUB

Whenever the lease has ended for a particular device, it's important to be certain all of your critical data is removed from the hard drive before it leaves the premises. Toshiba devices can be scrubbed to remove any and all information that may still be stored on the drive. We recommend an effective end-of-life policy up front.

You may choose to have Toshiba surrender the HDD to your authorize representatives to decommission as you see fit.

OUR INVITATION

If you have any questions or concerns regarding the security of Toshiba MFP's in your network we invite you to engage a Toshiba Business Solutions System's Solutions Engineer (SSE) to understand what options we can recommend to satisfy your current and future security strategy