TOSHIBA

e-BRIDGE Next

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

TOGETHER INFORMATION™

YOUR BUSINESS MAY BE AT RISK. TOSHIBA CAN HELP.

Protect Your Data and Your Business

Security is a growing concern for companies of all sizes. Toshiba employs innovative methods of protecting valuable data in order to help businesses of all sizes meet the increasing security challenges.

The Association of Certified Fraud Examiners found that companies in the United States lose more than $800 billion a year due to fraud, and document fraud is a large part of this statistic.[1] 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.

In a 2016 study, it was found that 35% of fraud was caused by purely insiders, while only 18% was caused by purely external sources.[2] The remaining is a combination of both sources. 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 $800 billion lost each year to fraud
- 1 in 3 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 2016 was $2.7 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.

[1] 2016 Global Fraud Study, Association of Certified Fraud Examiners
[2] Global Profiles of the Fraudster, KPMG International

TOSHIBA
Leading Innovation

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. 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 optionally FIPS 140-2 (Federal Information Processing Standards) certified, while the optional 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.

Document Management

Security is a top priority at Toshiba. That's why we protect critical data with exceptional, yet standard, security features. For instance, Private Print requires a secure password at the MFP control panel before printing. Multi-station Print requires the user to swipe a badge at any approved, convenient device to permit printing. Security Stamp adds a classified stamp to all documents copied or printed, providing traceability. In addition, many Toshiba MFPs contain electronic audit logs for each print, copy, scan and fax job sent to or from the MFP.

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 Stored Data
- Creates Secure PDF
- Controls Access
- Encrypt Scanned Documents

Toshiba's Security Toolkit

Standard with all Toshiba e-STUDIO Devices.

Device
- SNMP v3
- MAC Address Filtering
- Port restrictions
- Data Sanitization
- SSL
- IPv6
- IP Filtering
- SMB Signing
- IPsec*
- Data Overwrite*
- Advanced Encryption
- FIPS Certified*

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

Document
- Multi-Station Print*
- Security Stamp
- SecurePDF
- Private Print
- Audit Logs
- Encryption

*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.

Toshiba (Australia) PTY Limited
ABN 19 001 320 421

Building C, 12-24 Talavera Road,
North Ryde, NSW, 2113
Tel: 1300 794 202

New Zealand
32 Lunn Avenue, Mount Wellington
Tel: 09 570 8530

www.toshiba-business.com.au
www.toshiba-business.co.nz