

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

secureMFP™



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.

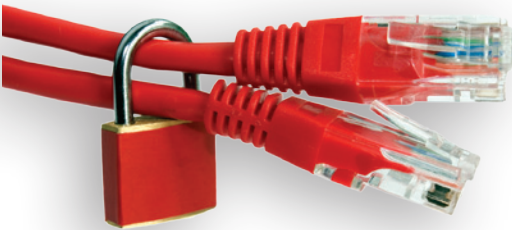
Protect your data and your business

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 2009 Data Breach Investigation Report found that 74% of security breaches resulted from external sources and 20% 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
- > 50%-70% of all identity theft occurs in the workplace



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.



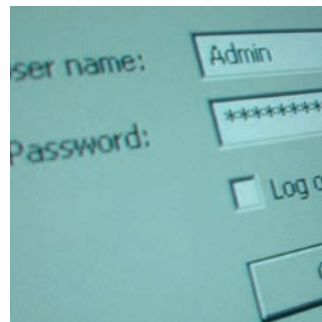
- Secures Print Output
- Protects Data
- Creates Secure PDF
- Controls Access

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** 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.



Control access to your MFP with Network Authentication.



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, Toshiba can offer the following solutions:

- **Private Print** prevents the wrong person from picking up the wrong print job and gives users the option of printing private documents individually or multiple documents at one time.
- **FollowMe® Printing** holds print jobs in a central queue until the user logs on to any FollowMe-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.

End of life security

When 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 end of life policy up front as part of your investment.



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

Every day,
billions of pages
of confidential
information --
medical records,
legal documents
and financial data
-- are produced
and distributed
using office copiers,
printers and MFPs.

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

Device

- SSL
- IPv6
- IP Filtering
- SMB Signing
- IPSec*
- Data Overwrite Kit*
- 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

*Optional security solutions

** Optional on some models

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

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.

Australian Head Office Building C, 12-24 Talavera Rd, North Ryde. NSW.
Tel: 1300 794 202 Fax: (02) 9815 6274
www.eid.toshiba.com.au

New Zealand 58 Lunn Avenue, Mt Wellington, Auckland
Tel: (9) 570 8530 Fax: (9) 570 8930
www.eid.toshiba.co.nz