TOSHIBA

Security Glossary

> The most important terms and
> features you need to know about.

ACCESS SECURITY

User/Department Codes

Not only do user codes control access, they also provide beneficial data tracking and usage information. User codes require users to enter a code in order to use the MFP device. Codes may be required for all walk-up functions, including copying, scanning and faxing, as well as printing from the desktop. Users are required to input a five-digit code either at the control panel for scan, copy or fax functions, or within the print driver when sending print jobs from a computer. Device administrators are able to easily track and view the volume and type of jobs being produced by each department or user. Additionally, these codes restrict unauthorised users from abusing company resources or gaining access to confidential information.

Strong Passwords

With the advent of password recovery tools that can crack passwords instantaneously, it is recommended that users create a strong password. A strong password is one that is at least eight characters, includes a combination of letters, numbers and symbols, and is easy for the user to remember, but difficult for others to guess. Unauthorised persons will find it difficult to access the administrative and network properties of each device, as well as to gain access to the device's control panel without the proper username and password. For further protection, a login limitation of up to three times can be employed. This sequence slows down the ability to crack the password by locking the screen after three failed attempts.

Usage Limitations

Usage limitations allow the administrator to control and track output at the device. With usage limitations, administrators can limit the number of copies or prints available at an account or a department level. The use of colour also is an optional restriction when dealing with a colour-capable device. This in turn provides a further level of security to complement the controlled device access, as well as the visibility to track and control costs associated with the device's use.

Network Authentication

For authentication, users are required to input their network user name and password to gain access to the control panel. Network administrators can control access to the device in the same manner that they control network access. If a user is authorised on the corporate network, then he or she can gain access to the MFP. Authentication ensures that only those users who have been authorised can gain access to data stored on the device. In addition, it lets e-mail recipients know the identity of the sender, deterring users from sending prohibited material.

E-mail Authentication

Authenticate natively with Microsoft Exchange e-mail servers.

Lightweight Directory Access Protocol (LDAP) Integration

LDAP provides a centralised address book of all employees and enables the administrator to establish rules and access rights based on specified user groups. For example, the administrator may prohibit employees employed by the company for less than 90 days from scanning or faxing. With LDAP authentication, the rules set by the administrator will apply to all MFPs on the company network.

Card Authentication

Card Authentication offers extensive security features designed to eliminate unauthorised operation and reduce costs and downtime. By utilising a streamlined, single point of entry, it facilitates the user log-in process by requiring a card swipe instead of typing a user name and password. With security taking a top priority among many companies, Toshiba is committed to providing solutions that ensure data integrity and accountability going to and from the MFP device. The administrator controls who has authorisation, thereby maintaining cost efficiency and security.

e-FOLLOW

A pull-printing solution for secure release of print jobs and effective print tracking and cost accounting.

DOCUMENT SECURITY

Secure PDF

Much like the private print feature, further control and protection are needed when scanning documents to e-mail and network locations. With Secure PDF, users can assign a password to scanned PDF documents directly from control panel of the MFP. The password allows for various levels of control such as access, printing, editing and copying the content. Furthermore, up to 128 bit AES encryption can be applied to ensure the document is protected. Secure PDF is the perfect solution for those wanting to email or store scanned documents without compromising the content.

Hard Copy Security

Embedded pattern print is a security function, which effectively restrains unauthorised copying and prevents the leakage of information by embedding hidden character strings during printing which reveal themselves when the document is copied. Example – Copying Prohibited.

Private Print

This functionality offers complete control of print output, requiring users to input a password before their document is output from the machine. When users walk up to the device to retrieve their document, they first have to enter their individually selected confidential password or present their authentication card. Only then will the documents sent by the user be released.

Toshiba also offers a batch private print feature to print jobs under the user's print queue. This eliminates the need to re-enter a password for each individual document if the user has sent multiple jobs. Private print is ideal for organisations printing confidential information, and prevents other people from accidentally or intentionally picking up the wrong print job. The private print feature is essential to controlling print data output at the MFP.

CERTIFICATES

Common Criteria Evaluated Assurance Level 3 (EAL 3)

The Common Criteria for IT Security Evaluation has different levels which describe in detail the requirements of an IT security inspection. The evaluation confirms that the security functionality stated by a manufacturer is valid. EAL3 evaluates the security behaviour of a device and uses development environment controls to confirm secure delivery procedures.

ISO/IEC 15408

Standard containing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation.

IEEE 2600.1 standards

Standard for a Protection Profile for Hardcopy Devices in a restrictive commercial information processing environment in which a relatively high level of document security, operational accountability, and information assurance, are required. Typical information processed in this environment is trade secret, mission-critical, or subject to legal and regulatory considerations such as for privacy or governance. This environment is not intended to support life-critical or national security applications.

DEVICE SECURITY

SSL
Secure sockets layer (SSL) is a cryptographic protocol widely used on the Internet to provide secure communications for transfer of personal information during online credit card transactions, order fulfilment, and accessing online accounts. MFP devices employ this common encryption technology to protect all data travelling 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.

IPv6
IPv6 is the latest version of IP and offers several features to address IP security needs such as:

> Increased address size
> Built in support for authentication
> Stronger confidentiality

IP Filtering
IP filtering essentially acts like a firewall to protect your internal network from intruders. IP filtering lets you control what IP traffic to allow into and out of your network by filtering data from specified network addresses. MFP devices utilise this mechanism as a means of controlling which computers have access.

SMB Signing
SMB (server message block) signing is a form of data authentication. During network authentication, once the MFP is authenticated on the server, SMB signing adds a digital signature to the data transferred between MFP and server. The signatures verify that the identity of the server matches the credentials expected by the MFP, and vice versa. By verifying that the data received comes from an authenticated source, the signature ensures the integrity of all communications.

IPsec
IPsec (IP Security Protocol) protects communication in the IP layer. It provides authenticated and encrypted submission of print jobs from desktop to a Toshiba MFP.

Advanced Encryption
Toshiba's innovative Secure Hard Disk Drive has set new security standards and provides ultimate security for sensitive data. The 256-bit AES encryption happens in near real-time and the encryption key is stored on the hard disc drive itself. Furthermore, the Toshiba Secure HDD knows which device it has been built into and requires the system to authenticate itself against the hard disc before allowing the data to be accessed. If this authentication fails, the encryption key will be deleted, guaranteeing that your data is safe.

Data Overwrite Kit
Data overwriting ensures that the hard drive is absolutely clear of readable data needed to process a print, scan copy or fax job. It works by overwriting the actual data with random and numerical characters. The disk is automatically cleared immediately after the device is done using the information after every job, thus preventing the data from being recovered by unauthorised users.