SHARP®

SECURITY SUITE

SHARP—A LEADER IN MFP & PRINTER SECURITY SYSTEMS

Our information and instant-communication world is filled with a vast array of technologies where all types of devices create, share, store, and transmit data. Technology plays a critical role, contributing to profitability in today's highly competitive business landscape and to the speed and richness of content available to personal communications. And while this has revolutionized the way in which we transact business and personal relationships, it has also created concerns for those who require that their information remain confidential and safe.

THE SHARP SECURITY SUITE

"The explosion of networked peripherals (hardwire or wireless) and mobile devices has added additional strain on IT to securely monitor and manage hardcopy peripherals ...".

"Authentication, authorization, and security remains the hottest subsegment ...".

"The picture in the United States resembles the worldwide forecast, with authentication, authorization, and security being the catalyst for high growth during the forecast period."

MARKET ANALYSIS: Worldwide and U.S. Document Solutions 2012 – 2016 Forecast, Ron Glaz
Source: IDC #238404

At Sharp Electronics Corporation, we are aware of the challenges in keeping our customers' data and information secure and free from malicious attempts to steal, illegally modify, intercept, or disseminate confidential documents, or gain unauthorized access to private and business networks. We are focused on protecting our customers' information assets from common vulnerabilities associated with unsecured MFPs and printers, including:

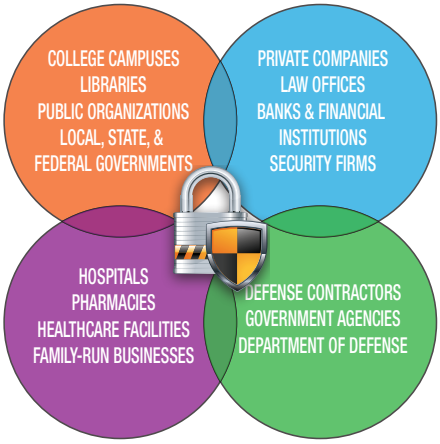
- Loss of productivity
- Regulatory non-compliance
- Loss of access
- Stolen information
- Lawsuits
- Unauthorized use of equipment and network resources

To address our customers' concerns we implement an iron-clad, multi-layered approach. The Sharp Security Suite provides protections that help ensure data and information security, access control security, network security, fax security, document security, and audit trail security.

We are proud of our long history of accomplishments in designing printers and MFPs that meet the most demanding security needs of our commercial and government clients. Sharp was a leader in addressing security in digital imaging and received the first Common Criteria Validation for an MFP in 2001. Today, Sharp remains a highly rated company and is regarded as one of the industry's greatest security innovators. Businesses and government agencies worldwide have come to depend on this level of assurance, which Sharp pioneered and for which it continues to set the benchmark.

Information in this brochure will provide you with a good understanding of Sharp MFP and printer security features and how you can implement these features to help protect your important information.

INTEGRATING MFP & PRINTER SECURITY INTO YOUR NETWORK



THE DRIVING FORCE—CRITICAL INFORMATION AND VERTICAL MARKETS

Security is important to any person who wants their data to remain confidential. MFP and printer security is of critical importance to IT organizations planning to place these devices on their networks. Their main concern is that the MFP or printer does not allow for malicious access to their network infrastructure and the data that courses through it. Sharp MFPs and printers offer exceptional security and peace-of-mind when it comes to protecting that data.

ORGANIZATIONS

College Campuses, Libraries, Public Organizations, Local Governments

CRITICAL INFORMATION

Student Records, Social Security Numbers, Addresses, Local Government Documents, Police Reports, Contracts, Legal Documents

Private Companies, Law Offices, Financial Institutions

CRITICAL INFORMATION

Employee Records, Payroll Information, Corporate Accounting and Financial Records, Tax Documents, Legal Documents, Case Information

Hospitals, Pharmacies, Healthcare Facilities

CRITICAL INFORMATION

Private Patient Records, Health Histories, Medication Records, Social Security Numbers, Treatment Records, Billing/ Payment Information

Defense Contractors, Government Agencies, Department Of Defense

CRITICAL INFORMATION

Classified Military Communications, Confidential Proposal and Bid Information, Military Contracts, Personnel Records, Payroll Information

INDUSTRY SPECIFIC CONCERNS

Ensuring data security and information confidentiality is often driven by IT security guidelines; however, certain types of organizations must employ security and information protection measures mandated by law, standards and regulating agencies, or by the federal government.

HEALTHCARE

Doctors, hospitals, insurance companies, nursing facilities, and other care providers must protect patient information, health histories, medication records, billing and insurance information, and other electronic healthcare transactions. Each of these entities must abide by the dictates of the **Health Insurance Portability and Accountability Act (HIPAA)**.

FINANCIAL

Banks, financial institutions, brokerage houses, and investment organizations are guided by the **Gramm-Leach-Bliley (GLB)** and **Sarbanes-Oxley Acts** to protect confidential records, transactions, and customer information.

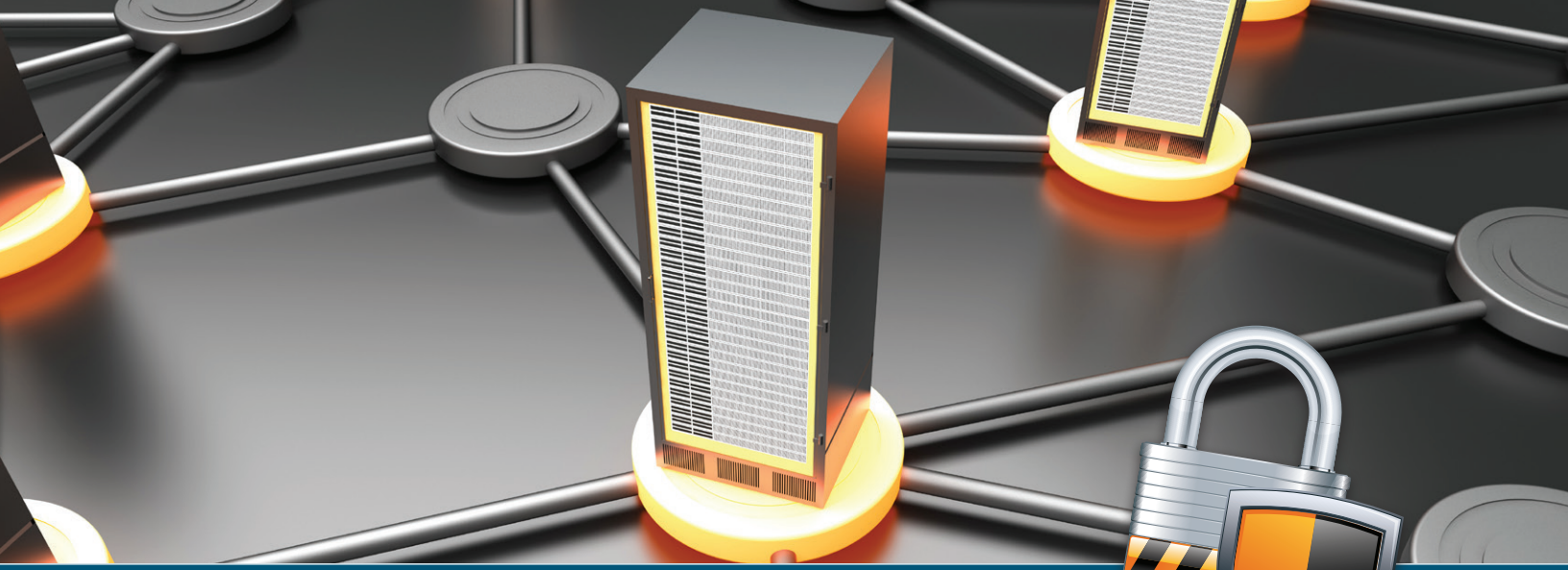
GOVERNMENT

Federal agencies, government offices, and defense department entities have strict data security mandates outlined in standards, specifications, and directives. Among the most stringent, and applicable to MFPs and printers are **ISO 15408 Common Criteria (CC) Evaluation Assurance Level (EAL)**, the **National Institute for Standards and Technology (NIST)**, and **Homeland Security Presidential Directive 12 (HSPD-12)**.

SECURITY CHECKLIST

Check Your MFP's Configuration—Help Ensure Maximum Security

- ✓ **Implement access control** (Active Directory® authentication, proximity cards, CAC, PIV cards and strong passwords).
- ✓ **Limit users who have administrator's rights**.
- ✓ **Change the MFP's administrator password** to something other than the default.
- ✓ **Close unused ports and disable unneeded network services and protocols**.
- ✓ **Use IP and MAC address filtering** to limit access to the MFP to only necessary PCs.
- ✓ **Install a Data Security Kit (DSK)** or configure built-in data security features.
- ✓ **Enable the SSL protocol as required** for HTTPS and IPPS web access and internet printing support.
- ✓ **Ensure that users are assigned to properly configured Authority Groups**.
- ✓ **Disable unused device functions**.
- ✓ **Periodically check job logs** for suspicious activity.
- ✓ **Enable POP3 and SMTP authentication** if possible.
- ✓ **Change the MFP's SNMP community name** from its default "public".
- ✓ **Do not "publish" an MFP's IP address outside your organization's firewall unless a very strong administrative password has been set**.



ADDRESSING THREATS

Security-conscious organizations will ensure that their network and computing assets are protected with the latest technology. Firewalls will be installed. Password rules will be enforced. User authentication will be required. Transmitted data will be encrypted and electronically signed.

The same security-conscious organizations will understand that today's intelligent multifunction devices (MFPs) and printers have evolved to have many of the same data communications and information storage capabilities found on personal computing devices that are already strictly controlled and secured.

These organizations will employ MFPs and printers that offer the advanced data, device, communication, and information security features found on Sharp equipment.

- **Hard Drive Overwrite**
- **Authentication**
- **Data Encryption**
- **Secure Networking Protocols**
- **Access Control**
- **Port / Service / Enabling / Disabling**
- **IP / Mac Address Filtering**
- **Encrypted PDF**

TYPICAL VULNERABILITIES AND SHARP'S COUNTER-MEASURES

WRONGFUL DISTRIBUTION OR VIEWING OF CONFIDENTIAL INFORMATION

Printed documents collecting in an MFP's output tray present a risk for unauthorized dissemination of critical information.

Sharp's MFPs help mitigate this issue with features such as print retention and user authentication.

IMPROPER ROUTING OF SENSITIVE INFORMATION

Legal contracts scanned to the wrong network folder may allow client data to fall into the wrong hands.

Sharp's latest generation of MFPs employs a scan-to-home feature that helps ensure that scanned images are stored appropriately.

UNAUTHORIZED ACCESS TO USER DATA STORED ON AN MFP

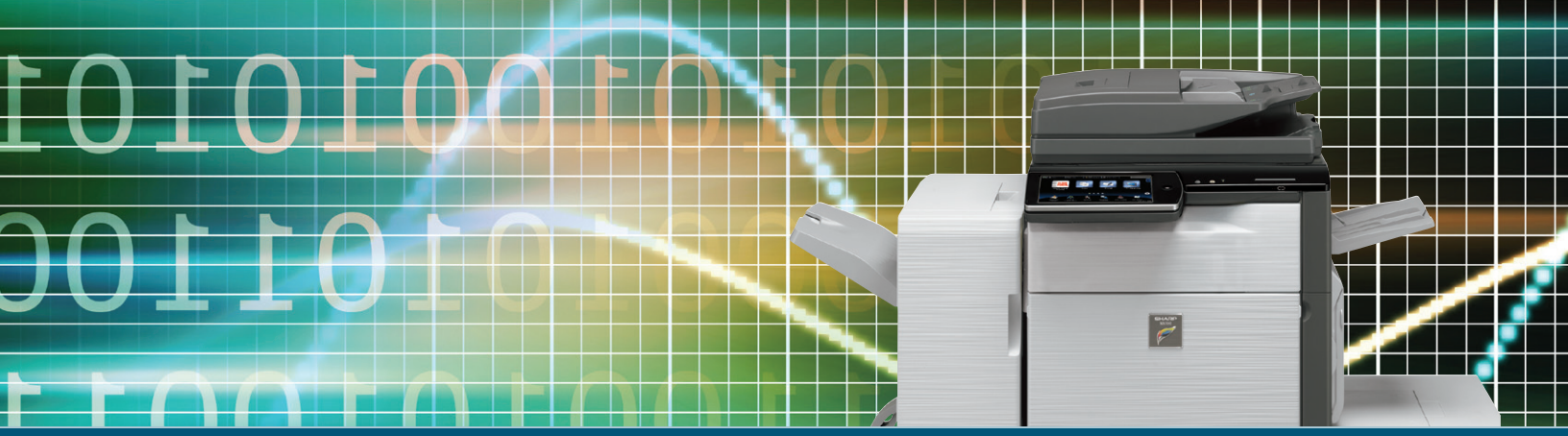
Persons with malicious intent may try to access sensitive user information and address book listings stored on an MFP's hard drive.

Sharp MFPs help address this threat with secure administrative passwords, IP and MAC address filtering, and multiple means of user authentication.

IMPLEMENTING ADDITIONAL SECURITY WITH SHARP'S DATA SECURITY KIT (DSK)

The information security needs of many environments will be met with the extensive standard security features available on Sharp's MFPs and printers. However, certain end-customers will require the additional security assurance provided by Sharp's Data Security Kit. The optional DSK brings device security to a higher level with features such as manual data overwrite and overwrite at power-up, CAC authentication (with an optional MX-EC50 Card Solution Kit), restrictions on the printing of lists that contain sensitive device and account information, and hidden pattern printing and detection.

And for MFP or printer placements in government offices, military bases, embassies, defense contractors, or anywhere that optimal security is required, Sharp's Common Criteria (CC) certified DSKs have been tested and certified to Evaluation Assurance Level (EAL) 3 according to the internationally-recognized ISO (International Standard Organization).



SECURITY FEATURES AT-A-GLANCE*

To help protect against physical and network security threats, Sharp MFPs and printers employ a multi-layered approach collectively known as the Sharp Security Suite. The security suite helps ensure that Sharp devices can be deployed with confidence as integral components within your information sharing infrastructure without compromising your company's security policies and practices.

Sharp's **MULTI-LAYER PROTECTIVE SECURITY SHIELD** consists of:

- **DATA & INFORMATION SECURITY**
- **NETWORK SECURITY**
- **DOCUMENT SECURITY**
- **ACCESS CONTROL SECURITY**
- **FAX SECURITY**
- **AUDIT TRAIL SECURITY**

DATA AND INFORMATION SECURITY

Sharp MFPs provide a wide range of data security capabilities either as an integral part of the device's architecture, or as a function of an optional Data Security Kit (DSK)

- Automatic Data Overwrite
- Manual Data Overwrite**
- Power-Up Data Overwrite**
- Up To 7-Times Data Overwrite
- 256-Bit AES Data Encryption
- End-Of-Lease Feature

ACCESS CONTROL SECURITY

Sharp MFPs can be configured to help provide iron-clad user access control.

- User Authentication (Local Address Book/LDAP)
- User Authentication (Global Address Book)
- Group Authorization
- Page Limit Control
- Secured Administrative Access to Device Home Page Administrator and User
- User Authority Setting
- Management of Currently Logged-In Users
- USB Card Reader Support
- CAC/PIV Authentication Capability**
- Scan-To-Home and Scan-To-Me
- Restrict List Printing**
- Disable Destination Selection
- Disable Address Book Registration
- Receipt Rejection from Specified Sender(s)

NETWORK SECURITY

Beyond simply protecting MFP access with passwords and various forms of authentication, Sharp MFPs support many methods of access control and means to "lock down" a device.

- SSL/TLS Encryption
- Security Policy Management (HASH Level Setting)
- SNMPv3 Support
- Kerberos Support
- SNMP Community Name Support
- IPv6 and IPsec
- Device Certificates
- IP Address Filtering
- MAC Address Filtering
- Port Control
- IEEE 802.1X™ Authentication

FAX SECURITY (Fax Option Required)

Customers who have Sharp MFPs equipped with the fax option can be assured that the architecture of the MFP provides a logical separation between the fax telephone line and the Local Area Network (LAN).

- Confidential Fax
- Segregated Fax Line from Network Connection
- Prevention of Junk Fax

DOCUMENT SECURITY

Protecting data on an MFP is only part of what's required to ensure complete end-to-end document security. Sharp MFPs employ a number of means to help assure customers that their document data will remain confidential.

- Secure Print Release with a PIN Number
- Encrypted PDF
- Encrypted PDF Lockout
- Tracking Information Print
- Hidden Pattern Print and Detection**
- Print Release Sharp OSA-enabled Applications
- MX-SW100 or Partner Program Applications
- Job Status Display Only For Logged-On User
- Secure Pull Print FTP/SMB

AUDIT TRAIL SECURITY

Sharp MFPs offer extensive internal logging, and in conjunction with the Sharp Remote Device Manager (SRDM) application, a large number of important job details can be tracked. Audit tracking is often a critical component requested in bids and solicitations. Information that Sharp MFPs can provide include:

- Job Log and Usage Tracking
- Reporting and Data Export In .CSV and .XML Formats
- Advanced Audit Trail Applications
- Program Partner Applications

** Based on security features of MX-2640N/3140N/3640N. ** Data Security Kit (DSK) feature.*

SECURITY FEATURE COMPATIBILITY (MONOCHROME)

	MX-B201D	MX-M232D	AR-M257/ 317	MX-M264N/ M314N/ M354N	MX-B402	MX-B402SC	MX-M283/ M363/M453/ M503	MX-M623/M753	MX-M904/ M1054/ M1204
General MFP Features/Functions									
Speed	20 ppm	23 ppm	25/31 ppm	26/31/35 ppm	40 ppm	40 ppm	28/36/45/50 ppm	62/75 ppm	90/105/120 ppm
Hard Disk Drive	—	—	—	Avail	Yes	Yes	Yes	Yes	Yes
Data Security Kit (DSK) & Common Criteria Certification				****			****		
Commercial DSK (Optional)	—	—	AR-FR24U/AR-FR25U	MX-FR37U	MX-FR26U	MX-FR27U	MX-FR23U	MX-FR22U	MX-FR38U
Common Criteria DSK (Optional)	—	—	AR-FR24/AR-FR25	MX-FR37	—	—	MX-FR14	MX-FR22	—
EAL Validation Levell	—	—	EAL3+	EAL3	—	—	EAL3	EAL3	—
Data and Information Security									
Data Overwrite (Auto)	—	—	DSK Feature	Std	DSK Feature	DSK Feature	DSK Feature	DSK Feature	Std
Data Overwrite (Manual)	—	—	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature
Data Overwite at Power-up	—	—	—	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature
Up to 7 times Overwrite	—	—	—	Std with opt. HDD	DSK Feature	DSK Feature	DSK Feature	DSK Feature	Std
256 bit Data Encryption	—	—	—	Std with opt. HDD	Std	Std	Std	Std	Std
End-of-Lease Erase	—	—	—	—	—	—	—	—	Std
Access Control Security									
User Authentication (Local Address Book)	Per account code	Per account code	Per account code	Std	Std	Std	Std	Std	Std
User Authentication (LDAP/AD)	—	—	—	Std	Std	Std	Std	Std	Std
Group Authorization	—	Per account code, Copy/Print	Per account code, Copy/Print	Std	Std	Std	Std	Std	Std
Page Limit Control	—	Per account code, Copy/Print	Per account code, Copy only	Std	Std	Std	Std	Std	Std
Secured Access to Device Home Page	Std with opt. NW Kit	Std with opt. NW Kit	Std	Std	Std	Std	Std	Std	Std
Password Management	Std with opt. NW Kit	Std with opt. NW Kit	—	Std with opt. HDD	Std	Std	Std	Std	Std
User Authority Setting	Std. Fixed setting	Std. Fixed setting	—	Std	Std	Std	Std	—	Std
Restrict List Printing	—	—	—	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature
Scan-to-Home	—	—	—	—	—	—	—	—	—
Scan-to-Me	—	—	—	—	—	—	—	—	Std
Disable Destination Method Selection	—	—	—	Std	Std	Std	Std	Std	Std
Disable Address Book Registration	—	—	—	Std	Std	Std	Std	Std	Std
Receipt Rejection from Specified User(s)	—	—	—	Std	Std	Std	Std	Std	Std
Lock Users After 3 Tries	—	—	—	Std	Std	Std	Std	Std	Std
USB Card Reader Support	—	—	—	Std	Std	Std	Std	Std	Std
CAC/PIV Authentication (Optional)									
Embedded Solution (MX-EC50)*	—	—	—	—	—	—	Yes	Yes	—
Print Retention (MX-EC50)	—	—	—	—	—	—	Yes	Yes	—
Scan-to-Self and Site (MX-EC50)	—	—	—	—	—	—	Yes	Yes	—
External Solution (DCL310S)*****	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
E-mail Encryption (Both)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digitally Signed E-mail (Both)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Network Security									
SSL/TSL Encryption	—	HTTPS/SMTP/POP3/LDAP	HTTPS, IPPS only	Std	Std	Std	Std	Std	Std
Security Policy Management	Std. Fixed setting	Std. Fixed setting	Std. Fixed setting	Std	Std	Std	Std	Std	Std
SNMPv3 Support	—	—	—	Std	Std	Std	Std	Std	Std
Kerberos	—	Std with opt. NW Kit	—	Std	Std	Std	Std	Std	Std
SNMP Communicty String Support	—	—	—	Std	—	—	—	—	Std
IPv6 and IPSec	—	—	Std	Std	Std	Std	Std	Std	Std
Device Certificates	—	Std with opt. NW Kit	Std	Std	Std	Std	Std	Std	Std
IP Address Filtering	Std with opt. NW Kit	Std with opt. NW Kit	Std	Std	Std	Std	Std	Std	Std
MAC Address Filtering	Std with opt. NW Kit	Std with opt. NW Kit	Std	Std	Std	Std	Std	Std	Std
Port Control (Disable /Enable ports)	Std with opt. NW Kit	Std with opt. NW Kit	Std	Std	Std	Std	Std	Std	Std
Admin Password Protection**	—	—	—	Std	Std	Std	DSK Feature	Std	Std
IEEE 802.1X Support	—	—	—	Std	Std	Std	Std	Std	Std
Fax Security (Fax Option May Be Required)									
Separation Between Fax and Network	Std	Std	Std	Std	Std	Std	Std	Std	Std
Confidential Fax	—	Std	Std	Std	Std	Std	Std	Std	Std
Filter Junk Fax	Std	Std	Std	Std	Std	Std	Std	Std	Std
Document Security									
Job Status Display Only Logged On User	—	—	—	—	—	—	—	—	Std
Secure Pull Print FTP/SMB	—	—	—	—	—	—	—	—	Std
Secure Print Release with a PIN Number	—	—	Std	Std with opt. HDD	Std	Std	Std****	Std	Std
Encrypted PDF Transmission	—	—	—	Std	Std	Std	Std	Std	Std
Encrypted PDF Direct Printing	—	—	—	Std	—	—	Std****	Std	Std
Hiden Secuirty Pattern Print	—	—	—	—	DSK Feature	DSK Feature	DSK Feature***	DSK Feature	DSK Feature
Hiden Secuirty Pattern Detection	—	—	—	DSK Feature	DSK Feature	DSK Feature	DSK Feature***	DSK Feature	DSK Feature
Audit Trail Security									
Job Log and Usage Tracking	—	—	—	Std with opt. HDD	Std	Std	Std****	Std	Std

Certain features and functions may require options.

* MX-EC50 requires Commercial DSK.
** Admin password can be protected when a Sharp MFP is accessed from FTP, preventing password leakage.
*** Supported only on "N" models.
**** Require optional HDD when it is not equipped.
***** DCL310S supports FIPS 140-2 certified CAC encryption (E-mail & Communication)

SECURITY FEATURE COMPATIBILITY (COLOR)

	MX-2615N/ 3115N	MX-2610N/ 3110N/ 3610N	MX-2640N/ 3140N/ 3640N	MX-C312	MX-C402SC	MX-4100N/ 4101N/ 5001N	MX-4140N/ 4141N/ 5140N/ 5141N	MX-4110N/ 4111N/ 5110N/ 5111N	MX-6240N/ 7040N	MX-6500N/ 7500N
General MFP Features/Functions										
Speed	26/31 ppm	26/31/36 ppm	26/31/36 ppm	31 ppm	40 ppm	41/50 ppm	41/51 ppm	41/51 ppm	62/70 ppm	65/75 ppm
Hard Disk Drive	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Data Secuirty Kit (DSK) & Common Criteria Certification										
Commercial DSK (Optional)	MX-FR40U	MX-FR30U	MX-FR41U	MX-FR29U	MX-FR28U	MX-FR11U	MX-FR42U	MX-FR33U	MX-FR36U	MX-FR43U
Common Criteria DSK (Optional)	—	MX-FR30	—	—	—	MX-FR11	—	MX-FR33	—	—
EAL Validation Level	—	EAL3	—	—	—	EAL3	—	EAL3	—	—
Data and Information Security										
Data Overwrite (Auto)	Std	Std	Std	Std	Std	DSK Feature	Std	Std	Std	Std
Data Overwrite (Manual)	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature
Data Overwite at Power-up	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature
Up to 7 Times Overwrite	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
256 bit Data Encryption	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
End-of-Lease Erase	Std	Std	Std	—	—	—	Std	Std	Std	Std
Access Control Security										
User Authentication (Local Address Book)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
User Authentication (LDAP/AD)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Group Authorization	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Page Limit Control	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Secured Access to Device Home Page	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Password Management	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
User Authority Setting	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Restrict List Printing	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature
Scan-to-Home	—	—	Std	—	—	—	Std	—	—	Std
Scan-to-Me	Std	Std	Std	—	—	—	Std	Std	Std	Std
Disable Destination Method Selection	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Disable Address Book Registration	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Receipt Rejection from Specified User(s)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
LockUsers After 3 Tries	Std	DSK Feature	Std	DSK Feature	Std	DSK Feature	Std	DSK Feature	Std	Std
USB Card Reader Support	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
CAC/PIV Authentication (Optional)										
Embedded Solution (MX-EC50)*	—	Yes	Yes	—	—	Yes	Yes	Yes	Yes	Yes
Print Retention (MX-EC50)	—	Yes	Yes	—	—	Yes	Yes	Yes	Yes	Yes
Scan-to-Self and Site (MX-EC50)	—	Yes	Yes	—	—	Yes	Yes	Yes	Yes	Yes
External Solution (DCL310S)***	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
E-mail Encryption (Both)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Digitally Signed E-mail (Both)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Network Security										
SSL/TSL Encryption	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Security Policy Management	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
SNMPv3 Support	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Kerberos	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
SNMP Communicty String Support	Std	Std	Std	—	—	—	Std	Std	Std	Std
IPv6 and IPSec	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Device Certificates	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
IP Address Filtering	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
MAC Address Filtering	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Port Control (Disable /Enable ports)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Admin Password Protection**	Std	Std	Std	Std	Std	Std	Std	Std	—	Std
IEEE 802.1X Support	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Fax Security (Fax Option May Be Required)										
Separation Between Fax and Network	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Confidential Fax	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Filter Junk Fax	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Document Security										
Job Status Display Only Logged on User	—	DSK Feature	Std	—	—	—	Std	DSK Feature	DSK Feature	DSK Feature
Secure Pull Print FTP/SMB	—	—	Std	—	—	—	Std	—	—	Std
Secure Print Release with a PIN Number	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Encrypted PDF Transmission	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Encrypted PDF Direct Printing	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Hiden Secuirty Pattern Print	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature
Hiden Secuirty Pattern Detection	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature	DSK Feature
Audit Trail Security										
Job Log and Usage Tracking	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std

Certain features and functions may require options.

* MX-EC50 requires Commercial DSK.

** Admin password can be protected when a Sharp MFP is accessed from FTP, preventing password leakage.

*** DCL310S supports FIPS 140-2 certified CAC encryption (E-mail & Communication).

SHARP ELECTRONICS CORPORATION
Sharp Plaza, Mahwah, NJ 07495-1163
1-800-BE-SHARP • www.sharpusa.com

Printed in U.S.A. 10/13 • CPD-3863