SECURITY SUITE TO SAFEGUARD YOUR BUSINESS

sharp security
generates confidence

version 2.2

TABLE OF CONTENTS

INCREASED SECURITY THREATS AND COMPLEXITY

Organizations of all sizes rely on a vast array of technologies to help make daily activities and communication more efficient. Adoption of new platforms such as mobile and cloud, can increase the frequency and complexity of security challenges. The more open and intricate these platforms become, the more corporations and organizations face constant threats that could put sensitive information and business continuity at risk. However, **implementing new technology is essential** to keep up with the speed of business.

Protecting sensitive data is crucial for business continuity.

Threat Types

Insider Security Breach

- Wrongful distribution or viewing of confidential information
- Improper routing of sensitive information
- Unauthorized access to data stored on the MFPs, folders and other services
- Lost laptops and mobile devices

Cyber Attacks

- Email containing malware and bots
- Email Phishing
- DDoS attacks
- Password hacks
- Malware and ransomware attacks through network and system vulnerability

New Risks – Third Platform

Mobile Adoption

- Data and network security vulnerability from BYOD
- Mobile OS vulnerability
- Malicious apps
- Infect mobile devices for monetization
- Misplaced mobile devices

Cloud Services

- Uncontrolled use of cloud services
- Business continuity and vulnerability challenges
- DoS attacks
- Cloud service hijack for ransom

INFORMATION SECURITY IN KEY VERTICAL MARKETS

New technologies such as mobile and cloud services are also transforming numerous vertical markets. However, when organizations adopt new communication platforms, data security and maintaining regulatory compliance become more challenging.

College Campuses, Libraries, Public Organizations

Education – The need for student privacy continues to grow as education records are digitized and shared electronically. Educational institutions must act responsibly, safeguarding students' personal data. Institutions must meet requirements of the Family Educational Rights and Privacy Act (FERPA) as well as the Health Insurance Portability and Accountability Act (HIPAA) on digitalized student information.

Critical Information: • Student Records • Social Security Numbers • Health Information

Defense Contractors, Government Agencies, Department of Defense, Local Governments

Local Government – Local government agencies maintain various types of data including social security numbers, credit card numbers, driver's license numbers, Federal Tax Information (FIT) and more. As the e-Government movement progresses, local government offices are under great pressure to protect sensitive information from hackers. Cybersecurity is one of the most critical components of IT for government agencies. Local government organizations, department entities, and courts, have strict data security mandates as outlined in several security standards, specifications and directives. Among the most stringent and applicable standards for MFPs and printers is ISO 15408/Common Criteria (CC) directed by National Information Assurance Partnership (NIAP).

Critical Information: • Social Security Numbers • Resident Information • Driver's License • Local Government Documents • Police Reports • Contracts

Lawyers, Law Offices, Service Organizations

Legal Services – Lawyers and law firms need to protect their client's data and information. In reaction to the rate of cloud and mobile adoption as well as the growing trend in data conversion requirements for e-discovery, companies offering legal services are forced to meet new regulations and compliances such as the EU General Data Protection Regulation (GDPR) and U.S. Personally Identifiable Information (PII). Proper data classification ensuring only authorized users access to the confidential data will be critical to minimize the impact on legal practices.

Critical Information: • Social Security Numbers • Contracts • Case Information • Client Information

Hospitals, Pharmacies,
Healthcare Facilities

Healthcare – The Health Information Technology for Economic and Clinical Health Act (HITECH) and Meaningful Use execution enabled rapid adoption of Electronic Health Record (EHR) systems. The U.S. Department of Health and Human Service (HHS) recognized that advances in electronic technology and digitalized patient records could further risk the privacy and security of confidential health information. The privacy and security protections for individually identifiable health information are strengthened under the rule and national standards of the Health Insurance Portability and Accountability Act (HIPAA). Doctors, hospitals, insurance companies, nursing facilities and other care providers must follow HIPAA to protect patient information, health histories, medication records, billing and insurance information and other electronic healthcare transactions.

Critical Information: • Private Patient Records • Health Histories • Medication Records • Social Security Numbers

Private Companies,
Financial Institutions

Financial/Corporate – Financial institutions and business organizations are constantly under threat of information leakage by internal and external sources. All organizations, regardless of size, that are "significantly engaged" in providing financial products or services, such as banks, mortgage lenders, brokerage houses and investment organizations, are guided by the Gramm-Leach-Bliley (GLB) Act to protect confidential records, transactions and customer information. In addition, all public companies need to comply with the Sarbanes-Oxley Acts (SOX). SOX mandates that organizations must store and track business information including electronic communications as well as hard copy documents. In addition, due to increased adoption of online transactions, corporations are required to meet new regulations such as GDPR. IT administrators are challenged to securely and cost-effectively store and manage all corporate and customer information.

Critical Informaton: • Customer Informaton • Employee Records • Bank Account Information • Corporate Accounting and Financial Records • Tax Documents • Credit Card Information • Social Security Numbers

PRINTER AND MFP SECURITY

Organizations are under constant threats from malicious attempts to steal and/or modify business data, or gain unauthorized access to their networks. Security threats as well as regulatory compliance requirements can be extended to the printers and Multi-Functional Printers (MFPs) that are commonly used in any organization.

Physical Security Threats

Typically, MFPs are located in common areas accessible by multiple people. Unauthorized personnel can potentially access and enter corporate networks when devices are not fully protected. In addition, any information stored on a local desktop computer or a server accessible through the network can be printed without authorization. Meanwhile, at the MFP device, confidential information can be accidentally or even purposely copied from stored documents, taken from the output tray or faxed without authorization.

Network Security Threats

Unsecured access to your company's stored data makes you vulnerable to having it stolen or altered. Furthermore, cyber criminals may obtain confidential information by unleashing a Denial-of-Service (DoS) attack, a phishing attack, or a virus via the network to launch an advanced cyber-attack. Phone line communications or network data could easily be intercepted when proper security measures are not implemented. Even MFP data stored on a hard disk drive or in memory could be compromised or stolen if not protected.

Protecting sensitive data is crucial and the end goal.

Today's intelligent MFPs and printers have evolved to include advanced network communications and data storage capabilities, failing to protect them may result in devastating damage to a company. Potential business impact includes:

- Loss of productivity
- Fines due to regulatory non-compliance
- Loss of access to data and network
- Loss of competitiveness due to stolen information
- Lawsuits

SHARP SECURITY SUITE

Sharp provides a multi-layered approach to help safeguard organizations against security threats. Sharp MFPs and printers are designed to help IT administrators and security officials plan, choose and implement proper risk prevention and control through the comprehensive Sharp Security Suite.

Sharp Security Suite includes:

- Standard MFP Security Features
- Data Security Kit
- Security Management Software
- Sharp Partner Program Member Applications

Achieve Optimal Security: Check Your MFP's Security Configuration!

- ✓ Implement secure user access control (Active Directory® or LDAP user authentication).
- ✓ Limit users who have administrator's rights.
- ✓ Apply more complex administrator password rules.
- ✓ Close unused ports and disable unneeded network services and protocols.
- ✓ Use IP and MAC address filtering to limit MFP access to only necessary PCs.
- ✓ Install a Data Security Kit (DSK) or configure built-in data security features.
- ✓ Enable the TLS protocol to secure all communications.
- ✓ Ensure that users are assigned to properly configured Authority Groups.
- ✓ Disable unused device functions.
- ✓ Periodically check job and audit 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.
- ✓ Ensure Wi-Fi and mobile security are properly configured.

Data Security in Transit or at Rest

Data security is a fundamental component for MFP and printer security. Sharp MFPs and printers include standard and/or optional security features that protect data stored on the device or in transition.

- **Data Encryption**

  When data encryption is enabled on a Sharp MFP, Advanced Encryption Standard (AES) algorithm 256 bit method is used in communication and on the data before it is written to RAM and the hard disk drive.

- **Data Overwrite**

  Up to 10 times programmable overwrite is used to maximize the data erase efficiency. The data is overwritten by random numbers. In addition, the data overwrite method can be customized to meet each organization's security requirements or it can be set as it is specified in DoD 5220.22-M.

Hassle-free erase/overwrite of data and settings completed securely.

Data Security Kit (DSK) and Common Criteria Certification/ISO-15408

Organizations may require enhanced security features to meet regulatory requirements or mitigate specific threats. Sharp's optional DSK brings device security to a higher level with features such as manual data overwrite and auto at power-up, hidden pattern printing and detection, and more. In addition, select DSK models are equipped with Trusted Platform Module (TPM) which helps further prevent unwanted access to data storage areas including hard disk drive and solid state drive.

- **Trusted Platform Module (TPM)**

  TPM is an industry standard computer chip with **crypto-processor technology**, integrating cryptographic keys to protect hardware such as Sharp MFPs and Printers. Sharp MFPs use an encryption key to protect the data including device certificates stored on non-volatile storage such as the **Hard Disk Drive** (HDD) and **Solid State Drive** (SSD). TPM stores a cryptographic key to authenticate and validate the platform, maintaining its trust while mitigating risk of data breach. TPM is an important component of the customers' trusted computing and network strategy and will greatly help protect them from data storage attacks on their Sharp MFPs.

The Common Criteria (CC) is a set of guidelines used to evaluate information technology equipment. It is the technical basis for an international agreement and the specification is tested by independent laboratories. Sharp has always aimed to achieve a secure and productive office environment through the development of our digital MFPs. Meeting evolving security standards, such as Common Criteria, are important to ensure organizations confidently handle the most sensitive data on Sharp devices. Recently Sharp achieved the industry's first CC certification against the latest **Protection Profile for Hardcopy Devices v1.0 (HCD-PP v1.0)**.

- **Protection Profile for Hardcopy Devices v1.0 (HCD-PP v1.0)**

  HCD-PP v1.0 (dated September 10, 2015) is a new requirement for multifunction printers (MFPs) based on the security requirements specified by the U.S. and Japanese governments, providing the most up to date security validation for businesses, government and military offices. It aims to protect the information processed by an MFP from security threats and includes specifications for encryption and firewalls. The HCD-PP v1.0 was developed through the industry collaboration with the National Information Assurance Partnership (NIAP) and the International-Technology Promotion Agency, Japan (IPA). HCD-PP v1.0 defines security for MFP as a whole and the "EAL" reference is no longer used.

Data Security at End-of-Lease

When the device is retired, it is important that the data retained within the device be removed or rendered in an unreadable format. Sharp document systems offer standard End-of-Lease features to ensure that all confidential data is overwritten before the device leaves the facility.

- **How is the data erased?**

  When the End-of-Lease feature is executed the data is overwritten up to 10 times. If DSK is installed or standard MFP security feature is enabled, the data is overwritten with random numbers. The amount of times the data overwrite occurs and custom overwrite methods can be configured.

- **What happens at the completion of End-of-Lease data erase?**

  While data is being erased, the data deletion progress will be displayed. After erasing is completed, the MFP will be rebooted automatically. The data erase completion report will then be printed out.

The following data will be erased using End-of-Lease data overwrite feature:

Setting Values	Job Image	User Input Data		System Data
• System Settings/Web Settings • Admin Password • Network Settings • Soft Switch • Product Key	• Job (image) Data on Each Mode • Unprinted Fax/Internet Fax/Direct SMTP Data • Document Filing Data • Data Stored in NAS Area • Image Data in Memory Box • Print Release Job Data	• Address Book • User Information (including User Index/User Count) • Job Program • Organization/Group List/Page Limit Group List/ Authority Group List/ Favorite Operation Group List • Billing Codes • Words Registered in Software Keyboard • Scanner Default Sender • Scanner Default Destination • Fax/I-Fax Forwarding Destination/ Sender/ Allow/Reject Sender	• Polling Protection Number • Dial-in Number • Auto Forward Table • Destination for Document Admin • Fixed Phrase (Text/Image Printing/ Subject/File Name/Body Text/Email Footer/Tracking Information) • Metadata Set • Custom Links • Sharp OSA Embedded Application • Custom Stamp/Custom Watermark • Color Profile • Download Font	• Job Status Completion Queue Data • Job Log • Encrypted Communication Control Information • Keyboard Input Character Translation Information

Sharp helps protect your data and personal information from the first day of operation to the time of trade-in.

Attack Prevention

Organizations are under constant threat of increasingly menacing cyber-attacks. Select Sharp MFPs are equipped with features that can help organizations prevent or better respond to such threats. IT administrators can proactively help combat these potential threats by enabling the following features:

- **Firmware Attack Prevention & Self Recovery**

  Select Sharp MFPs not only offer digitally signed firmware, but also have a built-in firmware recovery feature which will help minimize security risks associated with attacks on the device firmware. When the firmware recovery feature is enabled, the device tries to prevent and “heal” from firmware attacks by Intelligently comparing hash values to validate genuine ICU Main firmware. When validation fails, the Sharp MFP restores the firmware to previously validated firmware.

- **Application Whitelisting**

  Combating IT threats is more challenging when devices are connected to offer advanced features. In order to mitigate risks, Sharp’s whitelisting feature, available on select Sharp MFPs, can detect access attempts to the MFP’s file system and prevent unwanted access. When the source process is not in the whitelist, the whitelisting module denies nefarious access.

  - IT Administrators can be notified of whitelisting events via email or integrated with the organization’s Syslog or SIEM (Security Information and Event Management) systems using the MFP’s audit log feature.

Critical features that help organizations prevent threats.

User Authentication, Authorization and Restriction

Most Sharp MFPs can limit unwanted access with user authentication. All user credentials are transferred using a combination of Kerberos and Transport Layer Security (TLS) to help avoid interception. In addition, select models can be registered with Active Directory® domain offering Kerberos token-based Active Directory authentication. In addition, ID card authentication is supported on Sharp MFPs, providing a greater convenience for user authentication. "Secure mode" to request a user password upon logon is supported for ID card authentication, minimizing the risk of passwords being compromised.

User authentication types:

- Local user list
- LDAP
- Active Directory
- External authority with Sharp OSA®-enabled applications

User authentication methods:

- PIN number
- User name and password
- ID card

Sharp Security Suite helps mitigate threats through authentication and restriction.

Once the user is authenticated, access to certain features are either granted or restricted. IT administrators can securely and conveniently manage devices and access to specific features with an advanced level of control.

Key features for authorization and access restriction:

- Password protected admin access
- Print, scan, copy and fax function control
- Access control for MFP's HDD
- Page limit control
- Color printing restriction
- Forced pull printing
- Destination entry restriction
- Domain restriction
- Forced scan to logged-in users' email address
- Forced scan to logged-in users' home folder
- Security control and default setting using Active Directory Group Policy with Sharp ADM template files (Device settings and Print Driver settings)

Single-Sign-On (SSO) to Network and Cloud Resources

IT administrators often face challenges sustaining productivity while maintaining security. Select Sharp MFPs offer options for single-sign-on to add operational convenience while validating user access to the device and network.

When an MFP joins a domain, the MFP establishes trusted relationships with network resources. IT administrators can provide secure Kerberos token-based SSO to network and home folders as well as Microsoft® exchange server.

For Google Drive™ online storage service, Gmail™ webmail service and select cloud services, an OAuth token is used to establish SSO. Sharp provides IT administrators greater flexibility and options to provide convenience to users while maintaining organization's data and information security.

Single-Sign-On Supported Resources:

- Network folders and home folders
- Exchange server
- Gmail webmail service
- Cloud services (such as box™, Google Drive™, OneDrive® and SharePoint® Online)
- Sharp OSA® applications

Network Security

Network security is the fundamental process to protect organizations' network and resources from improper use, intrusions, denial-of-service (DoS) attacks and unauthorized access and modification. Sharp MFPs help IT administrators and security officers design comprehensive security environments to ensure only authorized parties and protocols are allowed to access their network with Sharp MFPs and printers.

- Network communication protection via TLS
- SHA-2 certificate
- Wireless LAN communication protection
- Secure protocols such as Kerberos, IPv6, and SMBv3
- IP address and MAC address filtering
- Port management
- Disable/enable features and functions
- SNMPv3 communication
- Device certificates
- CA Certificates
- IEEE802.1X™ authentication

Document Security

Protection for sensitive documents can be achieved through various document security features including encrypted Adobe® PDF files for scanning and printing and document filing features, which allow documents to be retained until they are needed – preventing unauthorized access to printed documents.

- Encrypted PDF
- Secure document filing features
- Pull printing/PIN printing
- Secure watermark

Email Security

Email is the most frequently used and critical business communication method at many organizations. Sharp MFPs offer various email security features to enhance data privacy capability to cultivate trust and reputation. For more integrated email security, select Sharp MFPs offer the Email Connect feature which establishes a direct connection for Exchange servers or Gmail. This also ensures the email is sent by the logged in user (not via the generic MFP address). The email containing the scanned document is then stored in user's sent folder. For the Exchange server, all server rules and security (e.g. size limit, destination restrictions) are automatically applied to scan-to-email maintaining the organization's email policy.

- Digital Signature and encryption with S/MIME
- Exchange server integration (authentication and restriction)
- Gmail webmail integration
- Send email from logged in user
- Store sent email on sent item folder
- Domain control
- Destination restriction

Enabling the mobile workforce safely and securely for on-the-go access.

Mobile and Wireless Security

Adoption of mobile technology is critical for organizations to be innovative and agile. However, IT administrators often face risks by allowing personal devices to access critical business information. Sharp provides optimal security for mobile users to connect with the corporate network via the MFPs and printers.

- User authentication (Active Directory, LDAP, Local User List, PIN number)
- SNMP security
- Print retention
- Serverless print release (select MFP models)

In addition, Sharp MFPs support “Access Point” mode which allows mobile users to connect via Wi-Fi for printing from and scanning documents to their mobile devices – without having to connect through the corporate network. The Access Point mode prevents data exchange between Wi-Fi and wired interfaces.

Audit Trail

Tracking user activities and events are important and helpful to maintain proper security measures. Granular audit trail and job log features from Sharp provide comprehensive auditing of all user activities and device events.

- **Job Log**

  Certain regulations require parameters, such as “to,” “from,” “when” and “file name” to be logged, reviewed and archived for conformance.

- **Syslog and Audit Log (Supports RFC 5424/3164 Standard Syslog Protocol)**

  With select Sharp MFPs, the IT team can monitor and review event logs such as when/what setting changes were made, or which IP addresses have accessed the device. Such events can be exported for further analysis or archiving. With the audit log feature, more granular event data including user authentication failure and firmware updates are captured. The MFP’s event log can be integrated with the organization’s syslog or SIEM (Security Information and Event Management) System to trigger immediate security alerts to IT administrators.

Print Security and IT Environment Compatibility

Printing is the most common daily task in many workplaces. An optimized printing experience is critical to maintaining productivity. At the same time, IT departments face increased demand for print security and compliance such as HIPAA and FERPA.

• Printing Standard and Compatibility

MFP compatibility with key IT environments is important for many organizations. Sharp MFPs and printers are tested and validated by major technology providers.

- WHQL certified print driver to ensure Microsoft compatibility to meet security standard in the Microsoft environment
- Citrix-ready evaluation to ensure Sharp MFP and printer performance in the Citrix environment
- Device types to ensure printing performance in the SAP® environment
- Healthcare application compatibility including Cerner® and McKesson

• User Authentication and Print Retention

When user authentication is enabled, all print jobs are authenticated and only validated print jobs are accepted on the device. In addition, with the Sharp document systems, users can send print jobs and store them on the MFP's hard disk drive, which can then be securely released using a PIN number or via user authentication. It also helps minimize waste from jobs abandoned at the printer.

Both serverless print release and print retention features are available to mobile users via the Sharpdesk® Mobile application to assist with mobile print security compliance.

• Serverless Print Release

To add more convenience with security, select Sharp MFPs can be designated as a print server, and have the job released on another supported machine that is on the same network. Users can simply walk up to the most convenient printer and securely release their print jobs. It is a standard feature on select MFPs and up to five client machines can be connected for this function.

OSA® Sharp Open Systems Architecture

• Sharp OSA-enabled Applications

For more advanced control, Sharp and the Sharp Partner Program community offer a broad selection of tightly integrated print release and output management software. For more information, please visit Sharp USA web site.

Fax Security

The architecture of **Sharp MFPs provides a logical separation** between the fax telephone line and LAN, helping to **prevent attackers from gaining access** to the internal systems of the MFP or the local network. Additional security features are incorporated such as disabling broadcasting, allowing and rejecting reception from specific numbers, user authentication and more.

- Logical separation between the fax telephone line and LAN
- Only fax protocol is permitted in Sharp's fax modem
- MFP architecture is designed to minimize the risk of transmitting malicious data (virus, etc.) to the main system.
  - UART (Universal Asynchronous Receiver/Transmitter) communication on Fax controller cannot control MFP controller.
  - Image transmission between FAX controller and MFP controller is also separated from UART communication.

TOOLS TO MAINTAIN YOUR MFP AND PRINTER SECURITY

Sharp continues to provide optimal security to its customers, immediately assessing newly discovered security threats and their impact. Security measures are often released via firmware or through application updates to maximize security provided by Sharp products. In addition, Sharp offers various tools to monitor and optimize MFP and printer security features.

SRDM enables administrators to take control of system features and simplify installation and management.

Sharp Remote Device Manager (SRDM)

SRDM is the ideal tool for IT administrators to efficiently manage and monitor their MFP and printer fleets to optimize device uptime. SRDM enables IT administrators to centrally manage, monitor and configure Sharp devices on their networks. This not only helps IT administrators manage devices, but SRDM also helps maintain optimal MFP and printer security. Using SRDM, IT administrators and security officers can create an MFP and printer security policy then centrally force the policy to devices on the network. When security settings are unintentionally altered, SRDM will notify administrator(s) or client incident management systems for them to immediately respond to potential security risks. Or, the SRDM intelligently resets security settings to defined security policy when any changes are detected.

Key SRDM features include:

- Manual or automated device discovery
- Device status and consumable monitoring
- Security policy management
- Scheduled power management
- Centralized administrator password management
- Remote front panel access for quick user assistance
- Email notifications
- Firmware management
- Device cloning and storage backup

Sharp OSA-enabled Applications

Sharp and the **Sharp Partner Program** community offer a broad selection of tightly integrated security features such as user authentication, authorization, print release and accounting. If you are interested in developing integrated security solutions to meet specific requirements for your organization, please visit the Sharp USA web site for more information.

SECURITY FEATURES AT-A-GLANCE*

DATA AND INFORMATION SECURITY

Sharp MFPs provide a wide range of data security capabilities 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**
- Custom and DoD 5200.22-m
- End-of-Lease Data Erase
- Power-Up Data Overwrite**
- Up To 10-Times Data Overwrite
- 256-Bit AES Data Encryption
- Trusted Platform Module (TPM)**
- Application Whitelisting
- Self-recovery Firmware
- Data Back Up

ACCESS CONTROL SECURITY

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

- User Authentication (Local/LDAP/Active Directory)
- Group Authorization
- Active Directory Group Policy
- Page Limit Control
- Password Protected Access to Device Home Page (Administrator and User)
- User Authority Setting
- Single-Sign-On (Kerberos and OAuth Token)
- Management of Currently Logged-In Users
- USB Card Reader Support
- ID Card User Authentication
- 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

Network security with MFPs and printers is one of the most critical concerns. Sharp offers various features to help protect organizations' IT network.

- TLS Encryption (2048 bit Key supported)
- Security Policy Management
- SNMPv3 Support
- SNMP Community Name Support
- Kerberos
- IPv6 and IPsec
- Device Certificates
- IP Address Filtering
- MAC Address Filtering
- Port Control
- IEEE 802.1X™ Authentication

EMAIL SECURITY

Send to email is one of the most common tasks for document scanning. Organizations can ensure secure send to email with Sharp MFPs.

- User Authentication
- S/MIME
- Send Only to Logged in User's Email Address
- Send from Logged in User (Email Connect)
- Store Sent Email on Sent Item Folder
- Apply Exchange Email Rules to Send to Email
- Single-Sign-On (SSO) (Kerberos and OAuth token)

FAX SECURITY

(Fax option may be 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).

- Segregated Fax Line
- Prevention of Junk Fax
- Confidential Fax

MOBILE AND WIFI SECURITY

Embrace mobile printing and scanning by eliminating unauthorized access to corporate network.

- User Authentication
- Print Retention
- PIN Number Printing
- Access Point WiFi Mode

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, that if implemented, can help assure customers that their document data will remain confidential.

- Secure Print Release with a PIN Number
- Encrypted PDF (AES 256 bit Encryption)
- Encrypted PDF Lockout
- Tracking Information Print
- Hidden Pattern Print and Detection**

PRINT SECURITY

Printing is the most common use of MFPs and printers. Sharp helps protect and secure print jobs during transition and at the printer.

- User Authentication
- TLS Encryption
- Secure Print Release with a PIN Number
- Serverless Print Release
- Sharp OSA Applications

AUDIT TRAIL SECURITY

Sharp MFPs offer extensive internal logging. Audit tracking is often a critical component to monitor user and device activity. Sharp MFPs can also provide the following information:

- Job Log and Usage Tracking
- Image Job Log
- Reporting and Data Export
- Administrator System Audit Logs
- Syslog Protocol RFC 5424/3164 for Syslog/SIEM Integration
- Program Partner Applications
- SRDM Security Policy Management Features

*Color Advanced and Essentials Series MFPs. **Optional Data Security Kit Feature.

Sharp Security Suite Compatibility (**monochrome**)

	MX-B350W/ B450W	MX-B350P/ B450P	MX-B355W/ B455W	MX-M364N/ M464N/ M564N	MX-M365N/ M465N/ M565N	MX-M2630/ M3050/M3550/ M4050/M5050/ M6050	MX-M3070/ M3570/M4070/ M5070/M6070	MX-M6570/ M7570	MX-M654N/ M754N	MX-M905	MX-M1055/ M1205 (without Fiery Option)
GENERAL MFP FEATURES/FUNCTIONS											
Speed	35/45 ppm	35/45 ppm	35/45 ppm	36/46/56 ppm	36/46/56 ppm	26/30/35/40/50/60 ppm	30/35/40/50/60 ppm	65/75 ppm	65/75 ppm	90 ppm	105/120 ppm
Hard Disk Drive	-	-	Std	Std	Std	Std	Std	Std	Std	Std	Std
DATA SECURITY KIT (DSK) & COMMON CRITERIA CERTIFICATION											
Data Security Kit (Optional)	-	-	MX-FR59U	MX-FR45U	MX-FR44U/FR44	MX-FR56U	MX-FR57U	MX-FR60U HCD PP (Protection Profile for Hardcopy Devices) v1.0 support	MX-FR47U/FR47	MX-FR54U HCD PP (Protection Profile for Hardcopy Devices) v1.0 support	MX-FR53U
Common Criteria Certification	Certified HCD V1.0 Dated 2015	-	Certified HCD V1.0 Dated 2015	Certified EAL 3	Certified EAL 3	Certified HCD V1.0 Dated 2015	Certified HCD V1.0 Dated 2015	Certified HCD V1.0 Dated 2015	Certified EAL2	-	-
DATA AND INFORMATION SECURITY											
Data Overwrite (Auto)	-	-	Std	Std	Std	Std	Std	Std	Std	Std	Std
Data Overwrite (Manual)	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Data Overwrite at Power-up	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Up to 10 Times Overwrite	-	-	Up to 10 times	Up to 7 times	Up to 7 times	Up to 10 times	Up to 10 times	Up to 10 times	Up to 10 times	Up to 10 Times	Up to 7 times
Custom Overwrite Pattern	-	-	User settable, DoD5220.22-M preset	-	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	-
256 bit Data Encryption	-	-	Std	Std	Std	Std	Std	Std	Std	Std	Std
End-of-Lease Data Erase	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Trusted Platform Module (TPM)	-	-	Yes	-	-	Yes	Yes	Yes	-	Yes	-
ACCESS CONTROL SECURITY											
User Authentication (local address book)	User Number	User Number	Std	Std	Std	Std	Std	Std	Std	Std	Std
User Authentication (LDAP)	-	-	Std	Std	Std	Std	Std	Std	Std	Std	Std
User Authentication (Active Directory)	-	-	Std	-	-	Std	Std	Std	-	Std	-
Group Authorization	-	-	Std	Std	Std	Std	Std	Std	Std	Std	Std
Page Limit Control	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Password Protected Access to Device Web Page	Yes	Yes	Std	Std	Std	Std	Std	Std	Std	Std	Std
Restrict List Printing	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scan to Home Directory	-	N/A	Std	-	Std	Std	Std	Std	Std	Std	-
Scan Only to Logged in User's Email	-	N/A	Std	Std	Std	Std	Std	Std	Std	Std	Std
Disable Destination Method Selection	-	N/A	Std	Std	Std	Std	Std	Std	Std	Std	Std
Disable Address Book Registration	-	N/A	Std	Std	Std	Std	Std	Std	Std	Std	Std
Receipt Rejection from Specified User(s)	Std	N/A	Std	Std	Std	Std	Std	-	Std	Std	Std
Lock Users After 3 Tries	Std (Ope panel only)	Std (Ope panel only)	Std	Std	Std	Std	Std	Std	Std	Std	Std
USB Card Reader Support	-	-	Std	Std	Std	Std	Std	Std	Std	Std	Std

continued on next page...

Items indicated with "Yes" in the table above may require additional options or software downloads.
* Admin password can be protected when a Sharp MFP is accessed from FTP, preventing password leakage. ** Supported only on "N" models. *** Requires optional HDD when it is not equipped.

Sharp Security Suite Compatibility (**monochrome**) *continued*

	MX-B350W/ B450W	MX-B350P/ B450P	MX-B355W/ B455W	MX-M364N/ M464N/ M564N	MX-M365N/ M465N/ M565N	MX-M2630/ M3050/M3550/ M4050/M5050/ M6050	MX-M3070/ M3570/M4070/ M5070/M6070	MX-M6570/ M7570	MX-M654N/ M754N	MX-M905	MX-M1055/ M1205 (without Fiery Option)
GENERAL MFP FEATURES/FUNCTIONS											
Speed	35/45 ppm	35/45 ppm	35/45 ppm	36/46/56 ppm	36/46/56 ppm	26/30/35/40/50/60 ppm	30/35/40/50/60 ppm	65/75 ppm	65/75 ppm	90 ppm	105/120 ppm
Hard Disk Drive	-	-	Std	Std	Std	Std	Std	Std	Std	Std	Std
NETWORK SECURITY											
AD Integration (Join Domain)	-	-	Std	-	-	Std	Std	Std	-	Std	-
TSL Encryption	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
2048 Certificate	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	-
Security Policy Management	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
SNMPv3 Support	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
SNMP Community String Support	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Kerberos	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
IPv6 and IPSec	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Device Certificates	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
IP Address Filtering	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
MAC Address Filtering	Std	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	Std
CSRF Measure	Std	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	-	-	Std	Std	Std	Std	Std	Std	Std	Std	Std
SHA-2	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
S/MIME	-	N/A	Std	-	-	Std	Std	Std	-	Std	-
FAX SECURITY (FAX OPTION MAY BE REQUIRED)											
Separation Between Fax and Network	Std	N/A	Std	Std	Std	Std	Std	Std	Std	Std	Std
Confidential Fax	-	N/A	Std	Std	Std	Std	Std	Std	Std	Std	Std
Filter Junk Fax	-	N/A	Std	Std	Std	Std	Std	Std	Std	Std	Std
DOCUMENT SECURITY											
Job Status Display Only Logged On User	-	-	Std	Std	Std	Std	Std	Std	Std	Std	Std
Secure Pull Print FTP/SMB	-	-	Std	Std	Std	Std	Std	Std	Std	Std	Std
Secure Print Release with a PIN Number	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Serverless Print Release	-	-	Std	-	-	Std	Std	Std	-	Std	-
Encrypted PDF Transmission	-	-	Std	Std	Std	Std	Std	Std	Std	Std	Std
Encrypted PDF Direct Printing	Std (w/o password)	Std (w/o password)	Std	Std	Std	Std	Std	Std	Std	Std	Std
Hidden Security Pattern Print	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Hidden Security Pattern Detection	-	-	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AUDIT TRAIL AND OTHER SECURITY											
Job Log and Usage Tracking	-	-	Std	Std	Std	Std	Std	Std	Std	Std	Std
Administrator Audit Log	-	-	Std	-	-	Std	Std	Std	Std	Std	Std
Digitally Signed Firmware	-	-	Std	-	-	Std	Std	Std	-	Yes	-

Items indicated with "Yes" in the table above may require additional options or software downloads.

* Admin password can be protected when a Sharp MFP is accessed from FTP, preventing password leakage. ** Supported only on "N" models. *** Requires optional HDD when it is not equipped.

Sharp Security Suite Compatibility (**color**)

	MX-C303W/304W	MX-C301W	MX-C300P	MX-C250/300W	MX-2651/3051/ 3551/4051	MX-3071/ 3571/4071	MX-2630N/3050V/ 3550V/4050V/ 5050V/6050V	MX-3070V/3570V/ 4070/5070V/ 6070V	MX-6580N/7580N (without Fiery Option)	MX-7090N/8090N (without Fiery Option)
GENERAL MFP FEATURES/FUNCTIONS										
Speed	30 ppm	30 ppm	30 ppm	25/30 ppm	26/30/35/40 ppm	30/35/40 ppm	26/30/35/40/50/60 ppm	30/35/40/50/60 ppm	65/75 ppm	70/80 ppm
Hard Disk Drive	Std	Std	-	-	Std	Std	Std	Std	Std	Std
DATA SECURITY KIT (DSK) & COMMON CRITERIA CERTIFICATION										
Data Security Kit (Optional)	MX-FR61U	MX-FR46U	-	-	MX-FR62U	MX-FR62U	MX-FR51U	MX-FR52U	MX-FR55U	MX-FR58U
Common Criteria Certification	Pending	-	-	-	Pending	Pending	Certified HCD V1.0 Dated 2015	Certified HCD V1.0 Dated 2015	-	-
DATA AND INFORMATION SECURITY										
Data Overwrite (Auto)	Std	Std	-	-	Std	Std	Std	Std	Std	Std
Data Overwrite (Manual)	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Yes
Data Overwrite at Power-up	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Yes
Up to 10 Times Overwrite	Up to 10 Times	Up to 7 times	-	-	Up to 10 Times	Up to 10 Times	Up to 10 Times	Up to 10 Times	Up to 10 Times	Up to 10 Times
Custom Overwrite Pattern	User settable, DoD5220.22-M preset	-	-	-	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset	User settable, DoD5220.22-M preset
256 bit Data Encryption	Std	Std	-	-	Std	Std	Std	Std	Std	Std
End-of-Lease Data Erase	Std	Std	-	-	Std	Std	Std	Std	Std	Std
Trusted Platform Module (TPM)	Yes	-	-	-	Yes	Yes	Yes	Yes	Yes	Yes
Whitelisting	Std	-	-	-	Std	Std	-	-	-	-
Firmware Attack Prevention & Self Recovery	Std	-	-	-	Std	Std	-	-	-	-
ACCESS CONTROL SECURITY										
User Authentication (local address book)	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
User Authentication (LDAP)	Std	Std	-	Std	Std	Std	Std	Std	Std	Std
User Authentication (Active Directory)	Std Group Policy	-	-	-	Std Group Policy	Std Group Policy	Std	Std	Std	Std
Group Authorization	Std	Std	-	-	Std	Std	Std	Std	Std	Std
Page Limit Control	Std	Std	Std	Std	Std	Std	Std	Std	Std	Std
Password Protected Access to Device Web Page	Std	Std	-	-	Std	Std	Std	Std	Std	Std
Restrict List Printing	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Yes
Scan to Home Directory	Std	-	-	-	Std	Std	Std	Std	Std	Std
Scan Only to Logged in User's Email	Std	Std	-	-	Std	Std	Std	Std	Std	Std
Disable Destination Method Selection	Std	Std	-	-	Std	Std	Std	Std	Std	Std
Disable Address Book Registration	Std	Std	-	-	Std	Std	Std	Std	Std	Std
Receipt Rejection from Specified User(s)	Std	Std	-	Std	Std	Std	Std	Std	Std	Std
Lock Users After 3 Tries	Std	Std	-	-	Std	Std	Std	Std	Std	Std
USB Card Reader Support	Std	Std	-	-	Std	Std	Std	Std	Std	Std

continued on next page...

Items indicated with “Yes” in the table above may require additional options or software downloads.
* Admin password can be protected when a Sharp MFP is accessed from FTP, preventing password leakage.   ** Only supports the file without a password.

Sharp Security Suite Compatibility (**color**) *continued*

	MX-C303W/304W	MX-C301W	MX-C300P	MX-C250/300W	MX-2651/3051/3551/4051	MX-3071/3571/4071	MX-2630N/3050V/3550V/4050V/5050V/6050V	MX-3070V/3570V/4070/5070V/6070V	MX-6580N/7580N (without Fiery Option)	MX-7090N/8090N (without Fiery Option)
GENERAL MFP FEATURES/FUNCTIONS										
Speed	30 ppm	30 ppm	30 ppm	25/30 ppm	26/30/35/40 ppm	30/35/40 ppm	26/30/35/40/50/60 ppm	30/35/40/50/60 ppm	65/75 ppm	70/80 ppm
Hard Disk Drive	Std	Std	-	-	Std	Std	Std	Std	Std	Std
NETWORK SECURITY										
AD Integration	Std Group Policy	-	-	-	Std Group Policy	Std Group Policy	Std	Std	Std	Std
TSL Encryption	Std	Std	HTTPS for client only	HTTP client only	Std	Std	Std	Std	Std	Std
2048 Certificate	Std	Std	Std	-	Std	Std	Std	Std	Std	Std
Security Policy Management	Std	Std	-	Yes	Std	Std	Std	Std	Std	Std
SNMPv3 Support	Std	Std	-	-	Std	Std	Std	Std	Std	Std
SNMP Community String Support	Std	Std	-	Yes	Std	Std	Std	Std	Std	Std
Kerberos	Std	Std	-	Yes	Std	Std	Std	Std	Std	Std
IPv6 and IPSec	Std	Std	Yes	Yes	Std	Std	Std	Std	Std	Std
Device Certificates	Std	Std	Yes	Yes	Std	Std	Std	Std	Std	Std
IP Address Filtering	Std	Std	Yes	Yes	Std	Std	Std	Std	Std	Std
MAC Address Filtering	Std	Std	Yes	Yes	Std	Std	Std	Std	Std	Std
Port Control (Disable/Enable Ports)	Std	Std	Yes	Yes	Std	Std	Std	Std	Std	Std
CSRF Measure	Std	Std	Std	-	Std	Std	Std	Std	Std	Std
Admin Password Protection*	Std	Std	-	Yes	Std	Std	Std	Std	Std	Std
IEEE 802.1X Support	Std	Std	-	-	Std	Std	Std	Std	Std	Std
SHA-2	Std	Std	-	-	Std	Std	Std	Std	Std	Std
S/MIME	Std	Std	-	-	Std	Std	Std	Std	Std	Std
FAX SECURITY (FAX OPTION MAY REQUIRED)										
Separation Between Fax and Network	Std	Std	-	Yes	Std	Std	Std	Std	Std	Std
Confidential Fax	Std	Std	-	Yes	Std	Std	Std	Std	Std	Std
Filter Junk Fax	Std	Std	-	Yes	Std	Std	Std	Std	Std	Std
DOCUMENT SECURITY										
Job Status Display Only Logged on User	Std	Std	-	-	Std	Std	Std	Std	Std	Std
Secure Pull Print FTP/SMB	Std	Std	-	-	Std	Std	Std	Std	Std	Std
Secure Print Release with a PIN Number	Std	Std	-	Std	Std	Std	Std	Std	Std	Std
Serverless Print Release	Std	-	-	-	Std	Std	Std	Std	Std	Std
Encrypted PDF Transmission	Std	Std	-	-	Std	Std	Std	Std	Std	Std
Encrypted PDF Direct Printing	Std	Std	Std**	Std**	Std	Std	Std	Std	Std	Std
Hidden Security Pattern Print	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Yes
Hidden Security Pattern Detection	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Yes
AUDIT TRAIL AND OTHER SECURITY										
Job Log and Usage Tracking	Std	Std	-	-	Std	Std	Std	Std	Std	Std
Admin Audit Tracking (SIEM and Syslog Integration)	Std	-	-	-	Std	Std	Std	Std	Std	Std
Digitally Signed Firmware	Std	-	-	-	Std	Std	Yes	Yes	Yes	Yes

Items indicated with "Yes" in the table above may require additional options or software downloads.

* Admin password can be protected when a Sharp MFP is accessed from FTP, preventing password leakage. ** Only supports the file without a password.

SHARP ELECTRONICS CORPORATION
100 Paragon Drive, Montvale, NJ 07645
1-800-BE-SHARP • www.sharpusa.com

3/19

Design and specifications subject to change without notice. Some images may be simulated.