



SHARP

Information Security Brochure

Information is the life-blood of every organisation /This is Why security is at the heart of Sharp.

No-one has endless resources /This is Why Sharp does more for you.

Simplifying your life

As an Information Technology professional, you are no doubt faced with a unique set of challenges that pull you in many different and often conflicting directions.

For example, almost everyone now has to do more with less – supporting disparate assets throughout the sprawling enterprise with maximum interoperability and minimal resources.

Internal security policies and government regulations impose strict requirements on protecting the confidentiality of personal information. And you probably also aspire to reduce the impact of your operations on the environment through reduced energy consumption and recycling.

At Sharp, we understand your goals and the issues that impede your ability to focus on strategic objectives. From developing award-winning Multi-Function Printers (MFPs) that incorporate impressive security capabilities and advanced document workflows to facilitating the administration of devices wherever you are, Sharp technology empowers productivity and protects your valuable data.

Sharp's security expertise is among the most respected, having pioneered the first and most comprehensive solution for MFPs. In addition, our innovative Sharp OSA development platform helps your MFPs reach further into your organisation and business processes and is supported by one of the largest developer communities in the industry.

Sharp is also a trusted leader in liquid crystal display (LCD) technology, from our line of BIG PAD interactive displays to ultra-slim bezel video wall monitors and high brightness digital signage displays.

And to help preserve the natural beauty of our environment, we have made a strong corporate-wide commitment to minimise the impact of Sharp products on our planet.

TECHNOLOGY YOU CAN DEPEND ON



Technology should work for you /This is Why our MFPs are so easy to use.

A comprehensive choice

We offer an array of MFPs and printers that can help you achieve a broad range of business objectives. From A3 and A4 workgroup MFPs to our light production MFPs, Sharp is redefining the role and importance of document technology in the workplace by offering products that are easy to use, customisable and secure.

Ease-of-use

Many other MFPs on the market have operation panels that force you to dig through layers of choices to find the features you need. Sharp MFPs offer an easy-to-use, tablet-like user interface combined with the industry's first integrated retractable keyboard, so you can enjoy intuitive control of even the most advanced functions. Yet another Sharp first was our duplex scan feature, which scans both sides of a document in a single-pass, providing increased efficiency and enhanced system reliability.

Customisation

The user interface of our MFPs can be customised with one-touch access to the functions, files or applications that are most important to you. Everything can be fully personalised, allowing you to add custom backgrounds and icons, change the display language and much more. In addition, the Sharp OSA Web services development platform, now in its fifth generation, provides advanced customisation capabilities to meet the unique needs of your business.

Security

MFPs can print, copy, scan and fax documents – any document – in seconds. They can also copy them to an easily concealed USB memory stick or distribute them via email and fax to any destination.

Sharp's award-winning security suite contains features to control usage and access, logging activity and erasing data after use, providing peace of mind and protection for your confidential and intellectual property, whether you are copying, scanning or printing.

NAVIGATE SMOOTHLY AND EASILY
ACCESS WORLD-CLASS FEATURES



Threats can appear anytime and anywhere /This is Why Sharp ensures you're always protected.

MFPs and printers are now a vital part of most organisations' document workflows and business processes, so they are a potential weak spot in your information and network security.

- **Physical security threats**

MFPs are usually located in common areas accessible by multiple people, so confidential information can be accidentally or deliberately copied from stored documents, taken from the output tray and scanned or faxed without authorisation. Unauthorised personnel can also potentially access and enter corporate networks when devices are not fully protected or securely configured. In addition, any information stored on a local desktop computer or a server accessible through the network can be printed without authorisation.

- **Network security threats**

Data stored on a hard disk drive or in the memory of an MFP can be compromised, altered or stolen if network access is not properly secured against unauthorised users. It could even be intercepted while being transferred over the network or Internet, when genuine security measures are not implemented. Furthermore, cyber criminals could obtain confidential information by unleashing a phishing campaign, a virus on the network or by hijacking an MFP to launch a Denial-of-Service (DoS) attack that targets your internal infrastructure or other external targets, using the Internet. Securing your MFP prevents your device from being used in an advanced cyber-attack.

- **Legal responsibilities**

Your company is legally responsible for the security of the data that it holds, wherever it is held, including employee records, customer information, account data, commercial information and sometimes much more.

Sharp recognises that securely managing business and user data is critical to your success – and survival. So we provide a suite of integrated security features designed to help protect your information and document assets from a multitude of threats, including the most sustained and determined attacks, while also meeting your legal compliance requirements:



PROTECT YOUR CONFIDENTIAL DATA
WITH THE SHARP SECURITY SUITE

The leader in digital information security

Sharp was the world's first MFP manufacturer to address security in digital imaging, receiving the first Common Criteria validation for an MFP in 2001 and being the first to achieve an EAL 4 rating for a data security kit. We are still recognised as one of the industry's greatest security innovators and continue to set the benchmark. Businesses and government agencies worldwide have come to depend on Sharp to keep their confidential data safe from unauthorised access.

The Sharp Security Suite

Sharp helps IT administrators and organisations achieve optimal document security. The Sharp Security Suite can prevent unauthorised access to your network and your most confidential information with safeguards that have been designed from the ground-up. Our MFPs utilise a multi-layered approach for protection – providing better control over the users, devices, ports, protocols and applications that access Sharp MFPs on your network.

The Sharp Security Suite includes:

- MFP security features as standard
- Enhanced Data Security Kit (Common Criteria Certified)*
- Print driver and software application security features
- Sharp OSA technology-enabled security applications

Data and information security

Sharp MFPs are equipped with a Data Initialisation/End-of-Lease feature. This protects your privacy by removing all data from the internal hard drive when it's time to replace your MFP.

For even greater data security, you can add our optional Data Security Kit (DSK), which was the industry's first Common Criteria certified solution of its type. The DSK protects and controls the major MFP systems and subsystems (print, copy, scan, and fax jobs, network settings, memory components and local user interfaces). The Advanced Encryption Standard (AES) 256 bit algorithm is applied to all data as it is written to the hard disk, SSD, RAM or Flash memory, helping to prevent successful attacks. The DSK also eliminates residual data by overwriting it up to ten times with a series of random values – either automatically on power on, automatically after each print, copy, fax or scan operation, or on user demand.

If your company handles sensitive information that would be an attractive target for skilled criminal hackers – such as credit card data – you may need to take extra precautions. An obvious, but often overlooked, step is to isolate the fax line. We've designed our MFPs in such a way that the fax modem controller is physically separate from the other controllers, so it cannot run any external code, and will only respond to genuine fax transmission protocols.



**Common Criteria
Validated**

MFP Data Security Kit

KEEP CONFIDENTIAL DATA SAFE
FROM UNAUTHORISED ACCESS

* Certification varies by MFP



MORE CONTROL MEANS
MORE PEACE OF MIND

Access control security

The first step in securing an MFP is to restrict who has access to it and what they can use it for. You don't have to make every function available to every user. The Sharp Security Suite controls walk-up access by authenticating the user. And we restrict network access with swipecards or a username/password combination authenticated against an LDAP or Active Directory Server. All user credentials are communicated to the MFP using a combination of secure protocols to help avoid interception.

Network security

Sharp MFPs feature an intelligent network interface that can limit access to specific computers on a network by IP or MAC address, and selectively enable or disable any protocol or service port on each device. All communications to and from the MFP can utilise SSL/TLS for secure transmission over the network, and most devices also support SMB, IPv6, IPSec, 802.1X and SNMPv3.

Fax security

The architecture of Sharp MFPs provides a logical separation between the fax telephone line and LAN. It therefore provides no path for attackers to gain 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.

Document and email security

Whether you're scanning, printing, or emailing, protection for sensitive documents comes as standard, thanks to Sharp's RSA encrypted Adobe PDF files, and use of SSL/TLS protocols and S/MIME email encryption for secure email communications.

Audit trail security

Sharp's more detailed audit trail and job log feature provides comprehensive auditing of all user activity. Certain government regulations parameters, such as "to," "from," "when" and "file name" can be logged, reviewed and archived for conformance. In addition, you can monitor and review event logs, such as when and what setting changes were made or which IP addresses have accessed the device.

Data and information security

- Data overwrite (auto)
- Data overwrite (manual and at power on)
- Up to 10 times data overwrite
- Custom and DoD 5200.22-m Preset Patterns
- 256-bit AES data encryption
- Data Initialisation/End-of-Lease feature

Access control security

- User authentication (device local/LDAP/Active Directory®)
- Group authorisation
- Page limit control
- Secured admin access to device home page
- Admin and user password management
- User authority setting
- Management of currently logged in users
- ID card reader support
- 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

- Active Directory Integration
- TLS encryption (supports 2048-bit certificate)
- 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
- Cross-Site Request Forgery (CSRF) measure

Fax security

(Fax option required)

- Confidential fax
- Segregated fax line from network connection
- Prevention of junk fax

Document security

- Secure print release with a PIN number/user authentication
- Serverless print release
- Encrypted PDF
- Encrypted PDF lockout
- S/MIME (Secure/Multipurpose Internet Mail Extensions)
- Tracking information print
- Print release Sharp OSA-enabled applications
- Job status display only for logged on user
- Secure pull print FTP/SMB

Audit trail security

- Job log and usage tracking
- Administrator audit tracking/ system log
- Reporting and data export in.csv and .xml
- Advanced audit trail applications

Additional Data Security Kit features (option)

- Self test function at power on
- Trusted Platform Module (TPM)
- Hidden pattern print and detection
- Firmware electronic signature check
- HCD PP conformance



UP TO TEN TIMES
DATA OVERWRITE

Security for small and medium-sized businesses (SMBs) and corporate organisations

Using the Sharp Security Suite, Sharp MFPs provide robust control over information access, transmission and tracking needed to meet stringent industry and legislative mandates – and avoid any penalties or lawsuits for non-compliance.

- Educational institutions
- Financial institutions
- Healthcare and Insurance providers
- Businesses across all industries can apply the strict controls over financial information required under the General Data Protection Regulation (GDPR).



Security for public sector and government organisations

Information sharing is critical for the efficiency of government and public sector organisations, but security management is becoming more challenging as the volume and complexity of attacks continues to grow. Sharp can help your organisation meet national and local government information security requirements through ISO 15408/Common Criteria certifications or comprehensive security features such as data encryption, Data Initialisation/End-of-Lease feature, administrator audit logs and more.

TURNING COMPLIANCE
INTO REAL ADVANTAGE



Data protection is continually evolving /This is Why Sharp helps you stay ahead of the game.

What is GDPR?

Businesses have always had a responsibility to protect the data they hold about their customers and employees, but on 25 May 2018 the European Union's new General Data Protection Regulation (GDPR) will replace legislation from the 1995 EU Data Protection Directive.

It's an important change, as the amount of data that businesses now store is vastly different to the data they stored in 1995. Search engines like Google, social networks like Facebook and digital marketing tools like Salesforce didn't exist in 1995, so the large volumes of data – Big Data – that these technologies generate was not adequately regulated.

Why GDPR is important

The aim of GDPR (formally called Regulation (EU) 2016/679) is to provide relevant regulation for today's digital world and protect the security of personal data that is now collected, stored, and used in previously unforeseen ways. For example, any online identifier, such as an IP address, now counts as personal data.

Under the GDPR, individuals can request a copy of any data that a business holds about them, and no data can legally be processed without their informed consent. This is to safeguard their rights as a 'data subject' and give them more say over how companies handle their data.

GDPR provides a real incentive to take data protection seriously as it features tougher fines for non-compliance and breaches. Failure to comply will incur a potential fine of up to €20 million or 4% of a company's annual turnover.

What GDPR means for SMBs

The GDPR will make data protection law the same across the EU, helping to create a simpler system, especially for multinational businesses. However, small and medium-sized businesses will also need to comply in full, just as they did with locally ratified versions of the EU Data Protection Directive.

As well as ensuring that they have an effective, documented, auditable process in place for the collection, storage, and destruction of confidential information, staff will need to be trained on the mechanics of the new regulation to help towards ensuring responsible data handling.



GENERAL DATA PROTECTION REGULATION

Assigning a Controller and Processor

In the GDPR, and in all data protection regulations, there are important distinctions about the responsibilities of different people or companies, depending on what they do with data.

The Controller is the person or company who makes decisions about processing activities, so they are the natural or legal person within your organisation who, alone or jointly with others, determines the purposes and means of the processing of personal data.

The Processor is contracted by the Controller to perform the processing of personal data on behalf of the Controller. As well as being another person in the same company, the Processor may also be another company that the Controller sub-contracts.

While the Controller is strictly responsible for personal data, the Processor has many obligations under the GDPR as well, which create significant liability if not performed diligently and effectively.

GDPR and document security

All businesses holding personal data, both Controllers and Processors, will need to have adequate security and back-ups in place to protect against potential attacks.

However, while a lot of the focus of the GDPR is on protecting online data, it also applies to physically stored data, which means that businesses need to consider what happens to the information that they print, copy, scan and fax.

Hard copies that are generated by an MFP and left on the output tray are vulnerable to unauthorised access. The digital information that passes through the printers and MFPs is a further security risk as residual data can be left behind and potentially retrieved by an attacker. And any printed documents that are left unattended or in unsecured recycling bins could be regarded as a breach of personal data.

Unsecure networked printers and MFPs could also be a point of risk. The digital copies of documents stored on them may become a target for hackers who want to steal information or they could be used as a platform to attack other systems.

How Sharp can help with GDPR

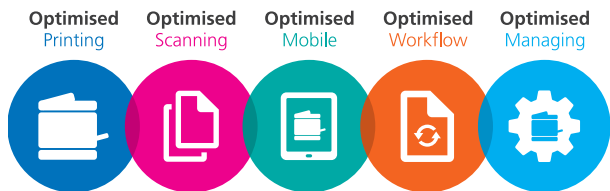
Sharp offers a wide range of security solutions that can help you ensure GDPR compliance, including security features built-in to Sharp's MFP hardware, secure print and document management solutions, and a cloud-based service for storing and sharing information.

Sharp's managed IT services, such as PC protection and secure back-up, also mean that we can help you protect your information, without putting any extra burden on your team, whatever the size of your business size.



PROTECTING PERSONAL DATA IN
PRINT AND DIGITAL FORMATS

The world is full of challenges /This is Why Sharp gives you optimised solutions.



At Sharp we believe there is always a solution for your ever changing business needs. So we offer a continually expanding range of innovative software that is designed to optimise the way you work – whatever your challenges or environment.

By building on the proven strengths of Sharp's MFPs, our portfolio of Optimised Software Solutions ensures that businesses can achieve even better:

- **Value** – reducing printing and copying costs with more control of usage and less wastage
- **Efficiency** – using internal resources and supplies more effectively with automated and consolidated management
- **Productivity** – making it easier to create, store and retrieve information using different devices, in any location
- **Compliance** – ensuring all actions are fully auditable, traceable and securely managed

OPTIMISING BUSINESS PRODUCTIVITY AND EFFICIENCY





Optimised Printing

Securely optimise your operating costs and ensure data integrity

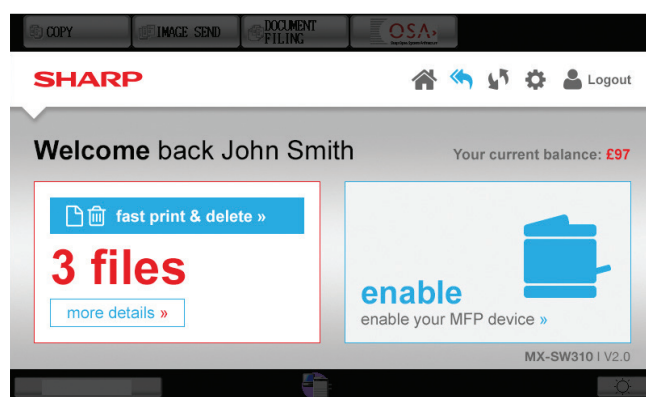
With Sharp's Optimised Printing Solutions you can securely access and release your documents when and where you need them.

In addition, you can proactively monitor, manage and allocate your print usage and costs with built-in billing code and print release features. Sharp MFPs and printers are also compatible with various output management applications, which offer simplified access-control and cost recovery features:

- **Access** – easy authentication via network username and password or ID card
- **Permissions** – control MFP function and feature access by user or by department to improve security
- **Visibility** – manage and monitor print/copy/scan activities to track spending and to optimise resources
- **Cost recovery** – bill clients back for the work you do for them

As well as delivering Follow Me Print / Secure Document release via PIN, Access Card, Active Directory or Two Factor Authentication (ID Card and PIN Number), printing can also be secured via print encryption (IPP via SSL/TLS) and endpoint encryption for data at rest. This can be used in conjunction with Sharp's MFP Data Security Kit for a complete end-to-end security offering.

VIEW YOUR BALANCE AND ENABLE YOUR MFP



SIMPLE & SECURE LOGIN



Optimised Scanning

Optimise your document management with data encryption and audit trails

Knowledge is key to every business's ability to innovate, operate and compete effectively. To unlock the real value of your information it has to be accessible by the right people, in the right place at the right time. And that means organising, storing and sharing documents effectively – however they are created or used.

Sharp's Optimised Scanning Solutions bring efficiency and control to the capture, distribution and management of your documents with automated processes for cleaning, annotating and indexing, which save time and prevent costly errors.

Digital documents, in file formats such as PDF, can also be encrypted, so they are kept secure when in transit using SSL/TLS channel encryption or at rest with document (PDF) encryption / password protection.



Optimised Workflow

Securely optimise your information sharing and enhance collaboration

Information is the lifeblood of any organisation, because the more you know, the better you perform. And optimising your document processes can increase your efficiency by up to 30%.

Sharp's Optimised Workflow Solutions help reduce costs and streamline repetitive tasks, restoring the business productivity you need to achieve and maintain profitable growth. Our cloud and on-premise solutions let you capture, store, manage, share and retrieve all of your business documents safely and securely. Any authorised user can access everything they need anytime, anywhere and on any web-connected device – enabling effective decision-making and effortless collaboration.

You can take digital documents from Line of Business (LOB) systems, and securely connecting these workflows to an array of software systems within your work environment. This can be on-premise or cloud-based services ensuring document communications are secure (via encryption) and compliant with relevant regulations.



Optimised Mobile

Securely optimise your mobile working with BYOD devices

The pace of business is accelerating and people now want to access information anytime and anywhere, using a wide range of mobile devices, such as smartphones and tablets. So you need a way for employees to quickly connect to your office devices wherever they are and whatever they are doing.

Sharp's Optimised Mobile Solutions provide Apps that link to your MFPs using any modern mobile device, regardless of whether they are internal systems or external Bring Your Own Devices (BYOD), such as mobile phones and tablets.

So you can easily and securely print, scan and share documents with other people and applications when you are on the move, harnessing encryption from the mobile device to the MFP, while still being able to manage and report on usage.

WORK FROM VIRTUALLY
ANYWHERE, ON ANY DEVICE





Optimised Managing

Ensure devices are constantly monitored and secured for optimum performance

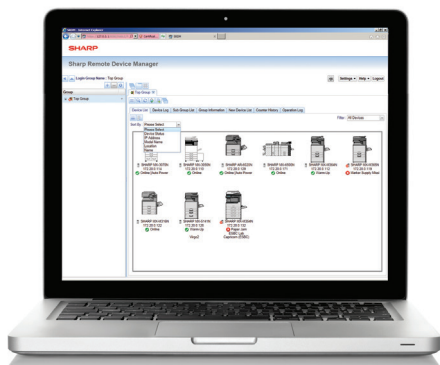
More than any other piece of office equipment, printers and MFPs demand continual attention – even if it's just to keep them supplied with toner and paper. And every time one becomes unavailable, the productivity of dozens of employees can be compromised.

Sharp's Optimised Managing Solutions are specifically designed to ease the burden of managing your fleet of MFPs, making your job easier and reducing the cost of ownership. Interruptions are minimised and downtime is reduced, while productivity is maintained across every workgroup in the company.

Effective tools to maintain your MFP and printer security

Sharp continually monitors emerging security threats and their impact. New security measures are often released via firmware or application updates to ensure that the most effective defences are always in place. In addition, Sharp offers various tools to monitor and optimise MFP and printer security features.

In particular, Optimised Managing enhances your security by enabling efficient device management, with proactive alerts, device settings configuration and device cloning capabilities. It allows your IT administrators to centrally manage all of your MFP / Print Driver Estate from a central location, reducing the overall administration time and resource effort.



MANAGE YOUR DEVICE, SAFEGUARD YOUR
DATA & PROTECT YOUR BUSINESS



EXPEDITE PROJECTS WITH REMOTE
FRONT PANEL ACCESS FROM ANYWHERE

Integration, customisation and personalisation with enhanced security

Sharp OSA technology is a software development platform for Sharp MFPs that is based on industry standard Web services/ Web API technology. It allows you to create integrated and customised interfaces that help streamline your business processes and extend access to mission critical information, while still ensuring that your IT network and security policies are maintained.

Sharp OSA technology for your organisation

Sharp OSA technology can help employees at every level of your organisation by optimising your IT investment, reducing costs, enhancing productivity and simplifying IT management:

Business owners, CEOs, COOs and CFOs

- Optimised investments in imaging systems
- Improved employee performance
- Compliance with industry regulations
- Cost reductions and optimised Sharp MFP capability

End customers and business process owners

- Instant productivity through engaging interfaces
- Intuitive and easy-to-use graphical user interface
- Simplified steps to process documents faster
- Seamlessly integrated daily document workflow

IT managers and administrators

- Integrated document and information security
- Improved access control, user management and usage tracking
- Integrated corporate IT assets and security policies
- Simplified management and support

Application developers and system integrators

- Extensive support and resources to accelerate development
- One of the strongest programs and developer networks in the industry
- Variety of resources available, including MFP simulator, documentation, developer hotline and more
- Wide range of programming languages supported on Web services/Web API and Webkit browser-based platform

Industry leader in Web services based MFP technology platform

Sharp pioneered the first Web services based MFP technology platform and, since the birth of Sharp OSA technology, we have been playing an important role in creating the industry's ecosystem. By developing strong connections among independent software vendors, solution providers and IT customers, Sharp has been helping organisations become more competitive in the marketplace.

Cloud-ready platform for intelligent IT decision making

Sharp OSA technology is cloud-ready, enabling your IT department to make intelligent and informed decisions when it comes to solution deployment. With RESTful Web API, Sharp OSA technology supports Software as a Service (SaaS) or cloud-enabled environments by efficiently assisting communications involving intermediaries, such as firewalls.

By enabling secure and scalable communications, Sharp OSA cloud-ready technology enables much greater flexibility in how document workflow and security solutions are implemented.

SCAN DOCUMENTS TO CLOUD PORTAL OFFICE FROM A SHARP MFP



Welcome to Sharp

Sharp Information Systems Europe (SISE), a division of Sharp Electronics Europe, offers a comprehensive portfolio of award-winning document management and display solutions to help organisations transform the way they engage with information. Sharp's industry-leading MFPs and light production systems sit at the heart of integrated applications for digital transformation.

Data Security

Sharp was the world's first MFP manufacturer to achieve Common Criteria certification and was also the first to receive EAL 4 for a data security kit. Data security continues to be a fundamental component of Sharp's MFPs and printers, with a range of standard and optional security features that are designed to protect data stored on the device or in transition.

Data Encryption

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

Data Overwrite

Up to 10 times programmable overwrite is used to maximise the data erase efficiency on Sharp MFP HDDs, with data being overwritten by random numbers. The optional data overwrite kit can be fitted to Sharp MFPs to ensure that your security complies with specific security criteria, such as DoD 5220.22-M.

Data Initialisation/End-of-Lease

When the device is retired, selected Sharp document systems offer Data Initialisation/End-of-Lease features to ensure that all confidential data is overwritten before the device leaves the facility. As the data is erased a "Now deleting (xx.x%)" message will be displayed with a progress indicator. If DSK is installed or the standard DSK feature is ON, the number of times erased will also be shown.

Notes

Design and specifications are subject to change without prior notice. All information was correct at time of print. Sharp, Sharp OSA is a registered trademarks of Sharp Corporation and/or its affiliated companies. Google is a registered trademark of Google Inc. All company names, product names, and logotypes are trademarks or registered trademarks of their respective owners. © Sharp Corporation October 2017. Ref: Information Security Brochure (18644). All trademarks acknowledged. E&OE.

SHARP

Inspiring ideas from technology

www.sharp.eu