Keep your business information secure

The comprehensive guide to document security in your office.

you can

Canon
How Canon keeps print environments secure

Control Restricted content leaving your organisation

The uniFLOW solution extends the security of information by checking printed, scanned, or faxed documents for restricted content and then informing an administrator of such a breach.

Printing confidential information leaves a trail

Job Log Guard removes all traces after confidential material is printed, so no trail is left.

Printer Hard Drive targeted by data thieves

Hard Disk Overwrite and Encryption* conforms with Common Criteria EAL3, giving you an internationally certified level of document protection. Removable HDD allows for the removal of the hard disk for storage in a secure location.

Hot-desking staff unable to keep confidential documents secure

Staff that don't have a mailbox can still ensure confidential material is not left exposed on a printer, by using the Secure Print option.

Unsecure personal and sensitive details

Personal Mailbox functionality means print jobs are sent to a folder on the hard drive of the device and retrieved for printing by the user.

Sensitive material left on the out-tray

Hot-desking staff unable to keep confidential documents secure

Unsecure personal and sensitive details

Personal Mailbox functionality means print jobs are sent to a folder on the hard drive of the device and retrieved for printing by the user.

Set Department IDs and passwords for up to 1000 departments and keep track of the copy, scan and print totals for each department.

Document security needs differ between individuals within businesses as well as between different businesses. Canon’s comprehensive approach to security ensures that all of these needs can be met across all the key areas of Confidentiality, Integrity and Availability.

This visual overview helps identify potential security risks within each of these areas and how Canon’s solutions address them using various layers of protection.

Confidentiality

IP and MAC Address Filtering ensures that only jobs from authorised computers/servers are printed.

Lack of control over which jobs are printed

With uniFLOW, you can route jobs to the most appropriate printer, plus you have a full document accounting system enabling you to track who is printing what and where.

Secure storage of Authentication and Security information

A Trusted Platform Module offers a secure storage location within the device hardware to hold authentication and security information.

User Management

Set Department IDs and passwords for up to 1000 departments and keep track of the copy, scan and print totals for each department.

Printing confidential information leaves a trail

UniFLOW allows jobs to be released by users at the device only if they are identified by proximity card, swipe card, PIN code or fingerprint ID.

Confidential documents ending up in the recycling bin

Confidential and Confidential Watermarks clearly mark sensitive information and discourage unauthorised copying.
The comprehensive guide to DOCUMENT SECURITY IN YOUR OFFICE

Contents

INTRODUCTION
How to use this guide 8
Why is security important? 10
Key security questions to consider 11
Security risks and tackling them 12
Prevalence of security breaches 14
Causes of security breaches 16

CONFIDENTIALITY
What is Confidentiality? 18
Document Protection 20
Information Transfer 24
Access Restriction 26
Secure Data Storage 32
Paper Output Control 36

INTEGRITY
What is Integrity? 40
Document Authenticity 42
Access Control 44
Usage Control 46

AVAILABILITY
What is Availability? 50
Document Protection 52
Software, Settings & Configuration 56
Access Control 58
Redundant System 64

SUMMARY
Standard Security Features 66
Additional Security Features 68
Glossary 70

Key solution’s focus

<table>
<thead>
<tr>
<th>Printing Documents</th>
<th>Scanning Documents</th>
<th>Managing Documents</th>
<th>Overlapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Protection</td>
<td>Information Transfer</td>
<td>Confidentiality</td>
<td>Access Control</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Integrity</td>
<td>Availability</td>
<td>Document Protection</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Confidentiality</td>
<td>Availability</td>
<td>Document Protection</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Confidentiality</td>
<td>Availability</td>
<td>Document Protection</td>
</tr>
</tbody>
</table>

Ensuring business critical information, from invoices to strategic plans and in physical or electronic formats, remains confidential.

Information remains true to the original version thanks to the control of changes or deletions by prior authorisation.

As well as being secure, we ensure that the information our customers need is available where and when required and in the right form.
An introduction to document security

Intellectual property, customer data, contract details, business strategies: there’s no end to the information at risk. That’s why it’s important to appreciate how these risks occur and importantly how they can be addresses with Canon solutions.

In Quocirca’s recent enterprise study, 52% of respondents indicated that printing is critical or very important to business activities with a further 24% indicating that printing plays an important if not essential role. Although many enterprises are failing to pay the same strategic priority to printers and MFPs. As a consequence, 70% of respondents indicate they have suffered one or more accidental printing-related data breaches.
How to use this guide

This guide looks at each of these key security areas in detail: **Confidentiality**, **Integrity** and **Availability**.

Each section throughout is clearly labeled and colour coded to make navigation easy. After an overview of security and the dangers posed, you’ll find each of the specific issues and their Canon solutions, split into three distinct areas.

What is in this guide?

This guide highlights all the issues and challenges faced today with clear explanations as to how Canon can address them. Independent research and useful press articles help explain issues from a different perspective.

To aid understanding, at the end of each section you will find “5 Key Points to Remember”.

---

**CONFIDENTIALITY**

Ensuring business critical information, from invoices to strategic plans and in physical or electronic formats, remains confidential.

Example: Encrypting information sent between PC and a device.

**INTEGRITY**

Information remains true to the original version thanks to the control of changes or deletions by prior authorisation. In many industries, ensuring the integrity of documents is a legal requirement.

Example: Applying user permissions so that an employee cannot delete confidential files.

**AVAILABILITY**

As well as being secure, we ensure that information needed by users is available where and when required and in the right form.

Example: Using controlled access at print devices.
Key security questions to consider

Many organisations will already have reasonable systems and policies in place that address security. But it’s just as likely that some areas aren’t been given due attention.

The following questions are worthy of attention by all businesses interested in the security of their information:

- Are you confident your print environment is secure?
- Have you ever considered the ramifications of losing data?
- What security policies do you have in your organisation?

Turn to the individual section on Confidentiality, Integrity and Availability to discover how Canon’s solutions can address these questions.
Security risks and tackling them

The security risks to organisations can be costly with severe repercussions. Only this year, the press has been littered with articles involving data security breaches and recent research has highlighted the average cost of these incidents to be as high as €1.8 million.

According to ENISA (European Network and Information Security Agency), “an uncontrolled printing environment is a major danger”.

1. Printers are no longer just printers
Multifunctional Devices (MFD’s) are actually servers in their own right, providing a number of networked services; for example email, file transfer (ftp), web and eFax servers, with some having significant hard drive storage as well. As such, they need to be treated in the same way, but are often not controlled to the same degree as corporate email servers or company web servers.

Organisations of all size should produce a configuration guide and ensure it is adhered to at all times. This will ensure all functions on the MFD are looked at critically and can be enabled or disabled as required.

2. Password protection is key
With the popularity of social networking in people’s lives, password theft has become even easier for malicious attackers. For example, password stealing Trojans and other malware can use fake password reset messages, which when activated then install on people’s machines. It has then been widely reported that one third of people use the same password for all websites and corporate accounts, meaning once the attackers have it they can access not only the individual’s personal data but also their professional information.

To ensure the MFD is a secure link in the information flow, organisations should disable default passwords and ensure employees have strong, unique passwords which are changed every 90 days for accessing their print jobs.

3. Paper based breaches are real
Nearly a quarter of security breaches are paper-based. Organisations can minimise the risk by using ‘Secure Job Release’, a function which means print jobs are locked in a queue on the device until the corresponding user PIN is entered. This will minimise the number of printouts left on the output tray, as documents will only be printed when they are required.

4. Insider threats are real
One of the ongoing risks for security professionals is not just the threat of malicious attacks, but the insider threat. Be it a disgruntled ex-employee leaking information for money or a well-meaning current employee, or simply human error – the risk of someone who has access to confidential information can be difficult to protect against.

By enabling the secure print options including ‘Secure Job Release’ outlined above, it protects from people stumbling on printed documents left on the output tray or illegally gaining access to an employee’s mailbox. It’s also important to consider what happens to the device at the end of its life. The hard drive of a printer must be erased and securely disposed of.
Prevalence of security breaches

A few years ago, the “National Survey on Data Security Breach Notification” was undertaken by Ponemon Institute, assessing both the prevalence and danger of such breaches.

The results were quite alarming:

Approximately 11.6% of survey respondents reported that they have received notification of a data security breach within the last year.

About 86% of security breaches involved the loss or theft of customer or consumer information. About 14% involved employee, student, medical and taxpayer data.

19% of respondents have already discontinued their relationship with the company as a result of the data breach.

So even a minor security breach could result in an almost 20% loss in customers. This is evidence enough to persuade organisations to have a cohesive policy in place, one that encompasses the entire security chain.

This guide shows you how Canon can help.
The Ponemon study also looked at the different causes of a security breach. The comprehensive guide to DOCUMENT SECURITY IN YOUR OFFICE

**Causes of security breaches**

The Ponemon study also looked at the different causes of a security breach.

- **Lost laptop or other device**: 36%
- **Paper records**: 24%
- **Third party or outsourcer**: 12%
- **Undisclosed**: 9%
- **Hacked systems**: 6%
- **Electronic backup**: 6%
- **Malicious code**: 3%
- **Malicious insider**: 3%

As you might have expected, lost or stolen laptops accounted for a significant proportion of breaches. However, the second most important, accounting for almost ¼ of the total, was security breaches associated with paper-based data.

"The fact that more than a third of breaches result from data being shared with third parties in the normal course of business is a clear signal that organisations should examine how they are sharing their customers’ data with outsourcers, vendors and partners."

Joseph Ansanelli, Vice President of data loss prevention solutions, Symantec.

**5 Key Points to Remember about Security**

- **Paper-based security breaches** are significant, accounting for 25% of all breaches.
- **86% of security breaches** involved the loss or theft of customer information.
- **Today’s printers** are actually sophisticated multifunctional devices providing numerous network services so should be protected in the same way as IT servers.
- Password protection is key as password theft becomes more common.
- Canon’s security solutions cover all the key areas of Confidentiality, Integrity and Availability.
What is Confidentiality?

Confidentiality is about making sure information in physical and digital format is not exposed or disclosed to unauthorised individuals or systems. The need for confidentiality spans numerous documents, covering anything from customer information to invoices to strategic business information.

Key areas of consideration are:
- Document Protection
- Information Transfer
- Access Restriction
- Secure Data Storage
- Paper Output Control.

Things to consider

- Did you know that 33% of office employees have seen confidential information on printers and copiers?
- How can you ensure that confidential documents aren’t lying around on the printer?
- Do you know that you can make sure only authorised personnel have access to certain documents?
- Do you know how to address the issues around intellectual property rights?
- Do you know it’s possible to create security protocols that respect HR policies in relation to the use of company information?
Document Protection

Causes of security breaches

Secure Watermark

The Secure Watermark functionality allows you to make copies and print documents with low visibility text embedded within the background. When the documents are copied, the low visibility text appears darker on the document. This is a visible deterrent against security leaks caused by the unauthorised copying of confidential information such as personal data, certificates and more.

eCopy File Encryption

This feature is standard with all editions of eCopy™ ShareScan®. eCopy ShareScan’s 128 bit File Encryption allows the user to encrypt scanned information (PDF files only), so that a password is required to open it. The password can be configured for length and type to comply with ‘strong’ password regulations. Once File Encryption is enabled, it can be set as mandatory or left as optional for the end user. File encryption can also be set on a per connector basis for every connection to back end systems.

File Usage

ShareScan’s File Encryption allows the user to set passwords for Adobe PDF documents to restrict opening, editing or printing a scanned document. Any recipient of the PDF document will be prevented from performing actions on the document unless they supply the correct password.

Encrypted PDF

The Encrypted PDF functionality encrypts the scanned image within a PDF before sending it from the device. This functionality is compatible with Adobe Acrobat standards and does not require a server to perform the encryption. Encrypted PDF restricts printing and text extraction via a password with up to 128 bit encryption.

Adobe LifeCycle Rights Management ES integration

With Adobe LifeCycle Rights Management ES integration, users can secure PDF files and apply persistent and dynamic policies to maintain their confidentiality, control their use and manage their availability. Users can closely monitor when and how often these files are accessed through detailed audit logs. The server allows users to control access and usage rights and protect sensitive and high-value information against inadvertent or malicious disclosure.

Since security policies are maintained at server level, users can change rights even after a file is distributed. To utilise this capability, Adobe LifeCycle Rights Management ES server and software needs to be installed and the imageRUNNER ADVANCE series needs to be connected to this server via internet or intranet.
Document Scan Lock & Tracking

This optional feature can embed Track & Lock code within copied or printed documents to restrict unauthorised copying, sending and faxing of these documents as well as track where these documents are originated. With this feature, users can set security restrictions on important documents to prevent others from duplicating copies, as well as sending or faxing these documents to unauthorised people. It embeds the “who copied/printed what at which device” information to track down a person who makes an unauthorised copy/print and identify the owner of a document even if it is left unattended.

Document Protection

iW Desktop print publishing tool allows you to also export to PDF and secure the file with a password. 128 bit encryption is used to ensure that only authorised people can view the contents of a document. This feature would be useful when distributing confidential information to a wider audience.

Note: this is available only on selected image RUNNER ADVANCE device ranges
Information Transfer

**Encrypted Printing**

The Encrypted Printing functionality encrypts the print job from the user’s PC to the MFP. A printer driver plug-in is required to encrypt the print data and the functionality needs to be activated on the device.

**eCopy Network Communication Encryption**

Standard with all editions of eCopy ShareScan

Network communications between the MFP and the ShareScan server is encrypted using HTTPS. This is the default setting and cannot be overridden by the user.

**IPSec Board**

The optional IPSec board allows users to use IPSec to ensure information privacy and security for the Internet Protocol (IP) communications over the network.

**What is IPSec?**

IP security is a suite of network layer protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream. It also includes protocols for cryptographic key establishment. It encrypts traffic so that the traffic cannot be read by parties other than those for whom it is intended, ensures that the traffic has not been modified along its path and is from a trusted party and protects against replay of the secure session.

**Protocol Configuration**

The Protocol Configuration allows the administrator to enable and disable the network protocols. The following protocols can be enabled and disabled:

- TCP/IP networking
- AppleTalk networking
- Novell (IPX) networking
- Windows (SMB) networking
- Dedicated Canon Port
- POP
- HTTP
- SNMP
- HTTP(S)

For all imageRUNNER ADVANCE models + imageRUNNER 32xx series

**SSL Certificates**

SSL Certificates are used to enable HTTPS functionality on the MFP. SSL Certificates provided by a Certificate Authority can be registered or you can generate a self certificate on the device. This allows information to be securely transferred when using either the remote user interface or MEAP applications on the MFP.

**IP And Mac Address Filtering**

The IP and Mac Address Filtering allows the user to block or allow specific IP or MAC addresses. The network administrator may want only 1 print server contacting the MFP. Therefore the MFP can be set up to only allow the print server’s IP or MAC address to contact it, blocking all other incoming network traffic.
Access Restriction

uniFLOW Login Manager

Optional module for all editions of uniFLOW
(Any edition of uniFLOW includes 1 module of choice for free.)
The uniFLOW Login Manager ensures only authorised users are given access to print documents from the print queues or a central document archive.

The uniFLOW Login Manager enables the Users to:
- Identify themselves at the MEAP enabled MFP.
- Select a Cost Centre by touching the display panel on the MFP.
- Securely hold their details (user name and email address) so that other applications on the device can use them.

Identification Methods

uniFLOW offers various ways of identification at the MFP:
- Entering a numeric code (e.g. a PIN-code), or an alphanumeric code (e.g. a cost centre)
- Using a magnetic card
- Using a contactless card
- Using your fingerprint.

MEAP Application

The display panel of the MFP is used to directly show information to the end users. The user does not have to move to another “add on 3rd party” device next to the MFP.

The MEAP application enables the Users to:
- Select one or more print jobs directly from users own secure personal queue and release it for printing.
- Select one or more print jobs directly from users secure group queue and release it for printing.
- Select one or more print jobs directly from a central document archive e.g. approved internal company documents or forms.

MEAP Application

Document Scan Lock & Tracking

This optional feature can embed Track & Lock code within copied or printed documents to restrict unauthorised copying, sending and faxing of these documents as well as track where these documents are originated.

With this feature, users can set security restrictions on important documents to prevent others from duplicating copies, as well as sending or faxing these documents to unauthorised people and embed the “who copied/printed what at which device” information to track down a person who makes an unauthorised copy/print and identify the owner of a document even if it is left unattended.

Security & Cost Control Pack proximity card authentication

Security & Cost Control Pack for Canon MEAP devices secures access to the device and secured print jobs via Job pin, username and password or even proximity card authentication.

Please note that Security & Cost Control Pack only supports Canon MiCard v2 HID contactless proximity cards. uniFLOW supports many more. Security and Cost Control Pack is a cost-effective solution suitable for small businesses with up to a maximum of 5 MFPs and 50 users. Above this the scalable uniFLOW Solution must be used.

Note: this is available only on selected imageRUNNER ADVANCE device ranges.
Thereof™ Access Rights For Documents

Access rights can be applied to most aspects of the system to define who sees which documents and who can open, edit, annotate, print etc.

Active Directory integration
Thereof™ integrates into the customer’s network infrastructure allowing existing security policies to be applied. Security administration is generally performed by managing Group Memberships in Active Directory.

Rights Server
Rights Server is an interface which a customer can implement using Thereof™ API/Developer Edition. It allows customers to apply non-standard access rights based on business processes.

For example:
Adding some delegate functionality, e.g. user A is out of office and user B should have all the permissions that user A normally has during this time.

A customer may have a special access table, defining which employee/user may access docs from which client, e.g.: employee A may access documents from clients 1, 2, 3; employee B manages relationship to clients 4, 5 and may see these documents. In the absence of employee A employee B would be given access to all documents relating to clients 1, 2, 3, 4 & 5.

iW Document Server Login - Access Privileges

Access privileges can be defined for all customer data via Access Control List (ACL). Only supervisors are allowed to change the settings of these access privileges. These include: Full Control, Right to Edit, Right to Update and Right to View.

The comprehensive guide to
 DOCUMENT SECURITY IN YOUR OFFICE

Department ID’s, SSO, SDL, S&CCP

Department IDs
Department IDs can be enabled on the MFP. The user enters their department ID code and password and can then make a print, copy, fax or scan. Without this ID code and password, the device functionality is unavailable.

Department ID codes can also have different access levels associated with them e.g. one code can allow users to copy and print in colour while another only allows users to make a black and white photocopy.

Department ID code usage limits (quotas) can be used to control usage of specific functions of the MFP. Separate limits can be set for the following functions:

- Total Prints
- Copy
- Scan
- Print

A breakdown of usage can also be printed if required.

Single Sign On (SSO)
Device security can be further enhanced using the Single Sign-On feature. By entering their network username and password, users can gain access to all the functionality of the multifunctional device (functionalities cannot be controlled individually).

Connection to the Active Directory ensures that only users who can log on to the network can also access the MFP. This also means that all changes made to the Active Directory by the IT department become immediately available to the MFPs, ensuring the same rights are maintained across the network.

To operate SSO, a Security Agent - acting as the interface between the MFPs and the Active Directory - needs to be installed on a server.

SSO-H
SSO-H is a login application that authenticates a user, either against a domain controller in an Active Directory environment or against a database on the local device. SSO-H locks down the device until the user has been authenticated. The key difference compared between SSO and SSO-H is that the latter no longer requires a Security Agent.

Simple Device Login (SDL)
If Active Directory is not available, users can still be made to “log in” to the Canon multifunctional device using SDL. With SDL, the user lists are stored on the device itself rather than the central active directory server. Users and groups can also be linked to department ID codes for centralised usage control.

The user management information for SDL is entered either via a web browser or can also be imported from a text file.

IEEE 802.1X
The 802.1X standard provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails.

IEEE 802.1X

The 802.1X standard provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails.
Secure Data Storage

uniFLOW Encrypt Job Name

Encrypt Job Name in Device Logs
Print Job Names are normally visible in shared print queues. A security kit is commonly applied to the device to hide the logs completely, however this disables accounting in most environments.

The Encrypt Job Name functionality replaces the Print Job Name and the User Name within a print job with a uniFLOW generated identifier. The print job names are no longer identifiable in the machine logs, eliminating the need for the security kit to hide the job logs.

Disguise Print Job Names
It is also possible to disguise the Print Job Names in order to prevent people from guessing the job’s content from a secure queue or job ticket queue in the spooler. The Job Names will be changed so that they are only identifiable by the uniFLOW system, which is meaningless to end-users.

eCopy Secure File Deletion

Secure File Deletion functionality deletes all temporary files on the server, overwriting each deleted file three times. This prevents individuals from retrieving files using data recovery tools.
This functionality complies with US Department of Defence standards.

Removable Hard Drive

The optional Removable Hard Drive Kit allows the removal of a hard disk for storage in a secure location. Using the kit, the hard disk can easily be removed and reinstalled easily and securely. Once installed, it can be secured by padlock.

Trusted Platform Module

The Trusted Platform Module (TPM) is an open standards security chip serving as a tamper-resistant storage vault for protecting highly sensitive information. Millions of laptops and desktops are shipped with TPM chips. It helps organisations harden applications against physical attacks.

Once the TPM chip is activated, it helps the device to protect against physical attacks. If it is removed from the device, it cannot launch, ensuring high levels of security controls.

The TPM can encrypt passwords, certificates, IDs and cryptographic keys. Encoded data on the hardware can be separated from passwords, certificates, IDs and cryptographic keys encrypted on the TPM chip.

Hard Drive Erase

The HDD Data Erase option is available for environments requiring additional data security. The kit will automatically overwrite and erase image data immediately after the job is completed; therefore, no trace of the data remains on the hard disk.

It will perform an overwrite up to 3 times with random data for maximum security protection depending on the preferences set by the system administrator. Other settings for the kit include the ability to overwrite once with null data and overwrite once with random data.
The comprehensive guide to DOCUMENT SECURITY IN YOUR OFFICE

Hard Disk Data Erase Kit

The Hard Disk Data Erase kit enables data that is no longer in use to be erased.

<table>
<thead>
<tr>
<th>Device</th>
<th>Data Erase</th>
<th>Data Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>iR32xx series</td>
<td>Data Erase Kit C1</td>
<td>HDD Data Encryption Kit B5**</td>
</tr>
<tr>
<td>imageRUNNER 6000 series</td>
<td>Data Erase Kit C1</td>
<td>HDD Data Encryption &amp; Mirroring Kit C2*</td>
</tr>
<tr>
<td>imageRUNNER 8000 series</td>
<td>Data Erase Kit C1</td>
<td>HDD Data Encryption &amp; Mirroring Kit C2*</td>
</tr>
<tr>
<td>imageRUNNER ADV C2000 series</td>
<td>Data Erase Kit C1</td>
<td>HDD Data Encryption Kit C3*</td>
</tr>
<tr>
<td>imageRUNNER ADV C5000 series</td>
<td>Data Erase Kit C1</td>
<td>HDD Data Encryption &amp; Mirroring Kit C1*</td>
</tr>
<tr>
<td>imageRUNNER ADV C7000 series</td>
<td>Data Erase Kit C1</td>
<td>HDD Data Encryption &amp; Mirroring Kit C1*</td>
</tr>
<tr>
<td>imageRUNNER ADV C9000 series</td>
<td>Data Erase Kit C1</td>
<td>HDD Data Encryption &amp; Mirroring Kit C1*</td>
</tr>
</tbody>
</table>

*Contains "Canon MFP Security Kit v2.00" complied to Common Criteria at EAL3 level
**Contains "Canon MFP Security Kit v1.50" complied to Common Criteria at EAL3 level

Job Log Conceal

This function enables you to hide the details of recent print jobs, concealing information like job name, type and date.

Hard Disk Data Encryption Kit

The Hard Disk Data Encryption Kit can be applied to the MFP to guarantee that the data on the HDD will be encrypted securely. HDD Data Encryption Kit contains the Canon MFP Security Chip 1.0/1.5/2.0 which is certified by ISO15408 (Common Criteria).
Paper Output Control

uniFLOW Secure Printing (incl. MyPrintAnywhere)

Optional module for all editions of uniFLOW. (Any edition of uniFLOW includes 1 module of choice for free.) uniFLOW Secure Printing provides users with effective security mechanisms to control the output of sensitive documents. Print jobs are held on the server and can only be retrieved at the MFP using an appropriate identification method. To allow for secure printing, user identification at the MFP is needed.

There are various configurations to suit different requirements:
1. Device Centric Secure Printing: The user prints the documents from their PC. The server holds the print jobs and releases them only when the user is identified at the MFP.
2. MyPrintAnywhere Secure Printing: The user prints the documents from their PC. The server holds the print jobs. The server releases the print jobs to any MFP at which the user provides a valid identification.

Identification Methods
uniFLOW offers various ways of identification at the MFP:
- Entering a numeric code (e.g. a PIN-code), or an alphanumeric code (e.g. a cost centre)
- Using a magnetic card
- Using a contactless card
- Using your fingerprint.

MicroMIND & MiCard devices use the MFP’s USB connection, thereby removing the requirement for an additional IP address. This reduces the points of attack on the network and the security concerns of another network attached device.

uniFLOW provides the administrator with an extensive set of configuration options to allow the system to integrate with existing customer environments.

uniFLOW is also designed to be customisable. Any new authentication devices, mechanisms or systems can be supported quickly and efficiently on a project basis.

iR Secure Printing

The Secure Printing functionality allows the user to set a numeric password within the printer driver during printing. The password must be entered at the device before the job can be printed.

iR Secure Mailbox

The Secure Mailbox functionality allows the user to print to a storage area (mailbox) on the device. The mailbox is password protected (by the user) and the user can gain access to these jobs by entering the password at the device.
Security & Cost Control Pack
Serverless Secure Printing

Security & Cost Control Pack for Canon MEAP devices includes a MyPrint Anywhere Secure Printing solution that allows users the flexibility to print securely from any MEAP device without the need of a Server. Proximity card authentication is also available to rapid and secure access to the device.

Security and Cost Control Pack is a cost-effective solution suitable for small businesses with up to a maximum of 5 MFPs and 50 users. Above this the scalable uniFLOW Solution must be used.

5 Key Points to Remember about Confidentiality

- Scanned documents and PDFs can be encrypted to prevent them being intercepted by unauthorised personnel.
- IPSec automatically ensures IP communications when information is passed between devices across the network.
- Canon’s uniFLOW ensures users must authenticate themselves at devices to prevent unauthorised access to information.
- Hard drives can be set-up to instantly erase information, as well as removed to allow secure and instant storage.
- The Security and Cost Control pack features MyPrintAnywhere allowing prints to be collected securely at the most convenient network device.
What is Integrity?

Integrity is achieved by ensuring that information cannot be altered or deleted without prior authorisation, keeping it “true” to its original form. With increasing numbers of digital documents, organisations need ways to effectively manage this.

This becomes more pressing as organisations seek to fulfil legal requirements concerning the integrity of their records.

Things to consider

• Do you know that you can create an audit trail of all the activities undertaken by print devices?
• There are often industry requirements concerning the handling of documents? How does your company adhere to these?
• Do you need to keep iterations of documents in your database?
• Did you realise that you can add a digital signature to all documents that you scan and thereby ensure the document cannot be altered by anyone?

Key areas of consideration are:

• Document Authenticity
• Access Control
• Usage Control.
The comprehensive guide to

DOCUMENT SECURITY IN YOUR OFFICE

Document Authenticity

Device Signature PDF
The Device Signature PDF Kit allows you to apply a digital (device) signature to each PDF file created at the MFP.

The user can select Device Signature PDF as the file type when scanning a document. The scanned document is converted into a PDF file and the digital device signature is added to the PDF file.

The digital device signature will show the recipient the email address of the user sending the PDF, which device sent plus the time, date and whether or not the document has been altered.

The digital certificates (from a certificate authority e.g. VeriSign) can be uploaded to the device via the remote user interface.

iW Desktop Digital Stamps
signed with Digital Certificates

iW Desktop a allows you to attach digital stamps to binder documents or PDF documents.

These digital stamps can be attached to e-documents as part of an electronic approval process. The digital stamps can be signed with a digital certificate to prove the authenticity of the annotation or digital stamp. iW Desktop supports digital certificates issued by Windows Server 2003/Windows Server 2008 as well as the VeriSign digital certificate.

Digital User Signature PDF Kit
The Digital User Signature PDF Kit allows you to apply a digital (user) signature to each PDF file created at the MFP.

The user can select User Signature PDF as the file type when scanning a document. The scanned document is converted into a PDF file and the digital user signature is added to the PDF file.

The digital user signature will show the recipient who sent the PDF, the time, date and if the document has been altered.

The digital certificates (from a certificate authority e.g. VeriSign) can be uploaded to the device via the remote user interface.

Therefore™ Digital Signature
Standard with all editions of Therefore™
The Digital Signature functionality assures users that the document displayed is exactly the same as the document which was originally saved.

Therefore™ Access Rights For Documents
Standard with all editions of Therefore™
Access rights can be applied to most aspects of the system to define who sees which documents and who can open, edit, annotate, print etc.

Active Directory integration
Therefore™ integrates into the customer’s network infrastructure allowing existing security policies to be applied. Security administration is generally performed by managing Group Memberships in Active Directory.

Rights Server
Rights server is an interface which a customer can implement using Therefore™ API/Developer Edition. It allows customers to apply non-standard access rights based on business processes.
Access Control

Therefore™ Access Rights For Documents

Standard with all editions of Therefore™

Access rights can be applied to most aspects of the system to define who sees which documents. This access control is achieved through user identification and only allows authorised users to access the documents.

Active Directory Integration

Therefore™ integrates into the customer’s network infrastructure allowing existing security policies to be applied. Security administration is generally performed by managing Group-Memberships in Active Directory.

Rights Server

Rights server is an interface which a customer can implement using Therefore™ API/Developer Edition. It allows customers to apply non-standard access rights based on business processes.

For example:

Adding some delegate functionality, e.g. user A is out of office and user B should have all the permissions that userA normally has during this time.

A customer may have a special access table, defining which employee/user may access documents from which client, e.g. employee A may access docs from clients 1, 2, 3; employee B manages relationship to clients 4, 5 and may see those documents. In the absence of employee A, employee B would be given access to all documents relating to clients 1, 2, 3, 4 & 5.

iW Document Server Login - Access privileges

Access privileges can be defined for all customer data via Access Control List (ACL). Only supervisors are allowed to change the settings of these access privileges.

These include: Full Control, Right to Edit, Right to Update and Right to View. User access can be managed locally or via Active Directory. iW Document Server uses Windows Internal Database (SQL Server Embedded Edition) SQL Server 2005 / SQL Server 2008.

Removable Hard Drive

The optional Removable Hard Drive Kit allows the removal of a hard disk for storage in a secure location. Using the kit, the hard disk can easily be removed and reinstalled easily and securely. Once installed, it can be secured by padlock.
Usage Control

**uniFLOW iWSAM Express Server and Secure Scanning Feature**

Administrators can capture an image of every print, copy, fax or scan that is made on the MFD via creation of an automatic log. Keyword recognition is supported for content monitoring and prevention.

Jobs can be searched for restricted keyword content and the administrator can be notified when restricted content is printed, copied, faxed or scanned by an unauthorised user. Furthermore, print jobs and scan jobs can be held before release to check for restricted keywords.

**uniFLOW Accounting & Statistics**

Optional module for all editions of uniFLOW.

(Any edition of uniFLOW includes 1 module of choice for free.)

The Accounting & Statistics functionality allows the accurate tracking and recording of all output from devices, inc. user, job name, and print information.

This allows administrators to monitor output for any potential abuse. It’s also possible to automatically schedule reports to be sent to key personnel.

**eCopy Activity Tracking**

Standard with all editions of eCopy ShareScan

eCopy ShareScan’s Activity Tracking can be configured to show a log of every scanned document, detailing who sent what and when. It is also possible to enable document tracking which saves a copy of the scanned document. When combined with the log, it provides a complete picture of what has been sent and by whom.

Managing access to appropriate functionality.
The comprehensive guide

**DOCUMENT SECURITY IN YOUR OFFICE**

---

**Therefore™ Access Rights For Documents**

- Standard with all editions of Therefore™
- Access Rights can be applied to most aspects of the system to define who sees which documents and who can **open, edit, annotate, print etc.**

**Active Directory Integration**

Therefore™ integrates into the customer’s network infrastructure allowing existing security policies to be applied. Security administration is generally performed by managing Group Memberships in Active Directory.

**Rights Server**

Rights Server is an interface which a customer can implement using Therefore™ API/Developer Edition. It allows customers to apply non-standard access rights based on business processes.

---

**iW Document Server Login - Access Privileges**

Access Privileges can be defined for all customer data via Access Control List (ACL). Only supervisors are allowed to change the settings of these access privileges. These include: Full Control, Right to Edit, Right to Update and Right to View.

**Access Management System (AMS)**

Optional on all IR devices

AMS uses the uniFLOW Login Manager to identify the user. AMS then enables or disables functionality on the device based upon the user.

AMS allows the administrator to:

- Control access to device functions based on users or group membership e.g. Guest users cannot send scanned information out to the internet (FTP, SMB, email is disabled), but normal users can.
- Hide functionality on the device to simplify the user experience, thereby reducing the risks of mistakes during use.

---

**Job Log**

The MFP contains a Job Log that is accessible via the Remote User Interface. The Job Log contains information about every Print, Scan, Fax etc that a user has made. The user name may be a Department ID or it may be the name of the person, depending upon the identification method used.

---

**5 Key Points to Remember about Integrity**

- **Integrity helps ensure information remains true to its original form.**
- **An Access Management System can be used to restrict access to specific device functionality e.g. guest users cannot scan and send information externally.**
- **Devices contain a job log detailing everything carried out.**
- **Administrators can capture an image of every print, copy, scan or fax made on a device.**
- **Restricted content (identified by keywords) can be highlighted to administrators should it ever be printed, copied, faxed or scanned.**

---
What is Availability?

Secure information needs to be readily accessible and instantly retrievable by those authorised to see it and in the format they expect.

Things to consider

- Do you know how it’s possible to ensure that users can always print what they need?
- Did you realise that simple to use encryption systems can make significant security improvements?
- Do you know how identification systems can be used that improve access to information as well as how it’s used?

Key areas of consideration are:

- Document Protection
- Software/Settings/Configuration Movement
- Access Restriction
- Redundant System.
Document Protection

The comprehensive guide to DOCUMENT SECURITY IN YOUR OFFICE

Having controls in place to secure the information within a document.

Secure Watermark

The Secure Watermark functionality allows you to make copies and print documents with low visibility text embedded within the background. When the documents are copied, the low visibility text appears darker on the document. This is a visible deterrent against security leaks caused by the unauthorised copying of confidential information such as personal data, certificates and more.

iR Encrypted PDF

The Encrypted PDF functionality encrypts the scanned image within a PDF before sending it from the device. This functionality is compatible with Adobe Acrobat standards and does not require a server to perform the encryption. Encrypted PDF restricts printing and text extraction via a password with up to 128 bit encryption.

eCopy File Encryption

Standard with all editions of eCopy ShareScan

eCopy ShareScan’s 128 bit File Encryption allows the user to encrypt scanned information (PDF files only), so that a password is required to open it. The password can be configured for length and type to comply with ‘strong’ password regulations. Once File Encryption is enabled, it can be set as mandatory or left as optional for the end user. File encryption can also be set on a per connector basis for every connection to back end systems.

File Usage

ShareScan’s File Encryption allows the user to set passwords for Adobe PDF documents to restrict opening, editing or printing a scanned document. Any recipient of the PDF document will be prevented from performing actions on the document unless they supply the correct password.
The comprehensive guide to DOCUMENT SECURITY IN YOUR OFFICE

Document Scan Lock & Tracking

This optional feature can embed Track & Lock code within copied or printed documents to restrict unauthorised copying, sending, and faxing of these documents as well as track where these documents are originated.

With this feature, users can set security restrictions on important documents to prevent others from duplicating copies, as well as sending or faxing these documents to unauthorised people and embed the “who copied/printed what at which device” information to track down a person who makes an unauthorised copy/print and identify the owner of a document even if it is left unattended.

Adobe LifeCycle Rights Management ES integration

With Adobe LifeCycle Rights Management ES integration, users can secure PDF files and apply persistent and dynamic policies to maintain their confidentiality, control their use, and manage their availability. Users can closely monitor when and how often these files are accessed through detailed audit logs. The server allows users to control access and usage rights and protect sensitive and high-value information against inadvertent or malicious disclosure.

Since security policies are maintained at server level, users can change rights even after a file is distributed.

To utilise this capability, Adobe LifeCycle Rights Management ES server and software needs to be installed and the imageRUNNER ADVANCE series needs to be connected to this server via internet or intranet.

Note this is available only on selected imageRUNNER ADVANCE device ranges.
Software, Settings & Configuration

**iW Management Console**

Free for download from Canon website

**Centralised Management of Printing Environment**

iWMC enables centralised management of a printing environment. iWMC enables device settings (protocol settings, Administrator contact details etc.), printer drivers, printer driver add-ins, resources (fonts, PCL macros, colour profiles etc.) to be “pushed out” to devices or users’ PCs by the IT Administrator. The centralisation of these tasks reduces the need for users to locate and install software themselves and this in turn reduces the risk of installing unsuitable or malicious software. This functionality allows IT Administrators to upload settings to the device and ensure security settings are kept consistent.

**Address Book Distribution (Address Book Plug-in)**

Device Address Books can be administered centrally by iWMC. The Administrator can create tasks to update and “push out” address books to devices on a regular basis. By doing this, the risk of users distributing confidential information by using out of date addresses (e.g. ex-employees), can be minimised.

**Printer Driver Distribution (Printer Driver Plug-in)**

Printer Drivers can be administered centrally by iWMC. Administrators can create tasks to distribute printer drivers to client PCs. Users can then install the latest drivers and patch releases and the risk of installing outdated or unsuitable drivers is reduced.

**User Authentication and Rights**

Access to the iWMC software and its various tasks is controlled by Local or Active Directory Authentication. Within iWMC, the Administrator can allocate rights to users or user groups to access menus and carry out tasks.

**System Logs**

The System Log tracks users actions including successful and failed log-in attempts.
Access Control

uniFLOW Login Manager

Optional module for all editions of uniFLOW.
(Any edition of uniFLOW includes 1 module of choice for free.)

The uniFLOW Login Manager controls the user access to the platform, therefore ensuring the availability only to authorised users.
The uniFLOW Login Manager uses the same technology as the MEAP Application, however it is used to secure access to all of the functions on the device and to identify the user at the device.

The uniFLOW Login Manager enables the Users to:
- Identify themselves at the MEAP enabled MFP.
- Select a Cost Centre by touching the display panel on the MFP.
- Securely hold their details (user name and email address) so that other applications on the device can use them.

Identification Methods
uniFLOW offers various ways of identification at the MFP:
- Entering a numeric code (e.g. a PIN-code), or an alphanumeric code (e.g. a cost centre)
- Using a magnetic card
- Using a contactless card
- Using your fingerprint.

MEAP Application
The display panel of the MFP is used to directly show information to the end users. The user does not have to move to another “add on 3rd party” device next to the MFP.

The MEAP application enables the Users to:
- Select one or more print jobs directly from users own secure personal queue and release it for printing.
- Select one or more print jobs directly from users secure group queue and release it for printing.
- Select one or more print jobs directly from a central document archive e.g. approved internal company documents or forms.

Security & Cost Control Pack
proximity card authentication

Security & Cost Control Pack for Canon MEAP devices secures access to the device and secured print jobs via Job pin, username and password or even proximity card authentication.

Please note that Security & Cost Control Pack only supports Canon MiCard v2 HID contactless proximity cards. uniFLOW supports many more.

Security & Cost Control Pack is a cost-effective solution suitable for small businesses with up to a maximum of 5 MFPs and 50 users. Above this the scalable uniFLOW Solution must be used.

eCopy Session Logon
Standard with all editions of eCopy ShareScan

eCopy ShareScan’s Session Logon locks the eCopy console so that a user has to enter credentials before being allowed access to the eCopy general user interface at the MFP.

This stops unauthorised use of the eCopy’s functionality and means users must log on with valid credentials before being able to scan.

uniFLOW Integration
The nT-ware Integration uses the uniFLOW Login Manager to identify the user at the device. The login information is securely passed to the eCopy application to provide essential user information for connection to other systems.

Users only have to authenticate once for both systems and have the ability to achieve this with the authentication system configured for the uniFLOW server.

Using only one authentication system is easier to manage and less of a security risk.
The comprehensive guide to
DOCUMENT SECURITY IN YOUR OFFICE

**Therefore™ Access Rights For Documents**

Standard with all editions of Therefore™

Access rights can be applied to most aspects of the system to define who sees which documents and who can open, edit, annotate, print etc.

**Active Directory Integration**

Therefore™ integrates into the customer’s network infrastructure allowing existing security policies to be applied. Security administration is generally performed by managing Group Memberships in Active Directory.

**Rights Server**

Rights Server is an interface which a customer can implement using Therefore™ API/Developer Edition. It allows customers to apply non-standard access rights based on business processes.

---

**iW Document Server Login - Access Privileges**

Access Privileges can be defined for all customer data via Access Control List (ACL). Only supervisors are allowed to change the settings of these access privileges. These include: Full Control, Right to Edit, Right to Update, and Right to View.


---

**For example:**

Adding some delegate functionality, e.g. user A is out of office and user B should have all the permissions that user A normally has during this time.

A customer may have a special access table, defining which employee/user may access documents from which client, e.g. employee A may access docs from clients 1,2,3; employee B manages relationship to clients 4,5 and may see these documents. In the absence of employee A employee B would be given access to all documents relating to clients 1,2,3,4 & 5.
Removable Hard Drive

The optional Removable Hard Disk Kit allows the removal of hard disk for storage in a secure location. Using the kit, the hard disk can easily be removed and reinstalled easily and securely. Once installed it can be secured by a Padlock.

Access Management System (AMS)

Optional on all iR devices
AMS uses the uniFLOW Login Manager to identify the user. AMS then enables or disables functionality on the device based upon the user.

AMS allows the administrator to:
Control access to device functions based on users or group membership e.g. Guest users cannot send scanned information out to the internet (FTP, SMB, email is disabled), but normal users can. Hide functionality on the device to simplify the user experience, thereby reducing the risks of mistakes during use.

Department ID’s, SSO, SDL

Department IDs
Department IDs can be enabled on the MFP. The user enters their department ID code and password and can then make a print, copy, fax or scan. Without this ID code and password, the device functionality is unavailable. Department ID codes can also have different access levels associated with them e.g. one code can allow users to copy and print in colour while another only allows the user to make a black and white photocopy. Department ID code usage limits (quotas) can be used to control usage of specific functions of the MFP. Separate limits can be set for the following functions:
- Total Prints
- Copy
- Scan
- Print

The counter information collected by using department IDs, including a breakdown of usage, can be printed if required.

Single Sign On (SSO)
Device security can be further enhanced using the Single Sign-On feature. By entering their network username and password, users can gain access to all the functionality of the multifunctional device (functionalities cannot be controlled individually).
Connection to the Active Directory ensures that only users who can log on to the network can also access the MFP. This also means that all changes made to the Active Directory by the IT department become immediately available to the MFPs, ensuring the same rights are maintained across the network.
To operate SSO, a Security Agent, acting as the interface between the MFPs and the Active Directory, needs to be installed on a server in the customer environment.

SSO-H
SSO-H is a login application that authenticates a user, either against a domain controller in an Active Directory environment or against a database on the local device. SSO-H locks down the device until the user has been authenticated. The key difference compared between SSO and SSO-H is that the latter no longer requires a Security Agent.

Simple Device Login (SDL)
If Active Directory is not available, users can still be made to “log in” to the Canon multifunctional device using SDL. With SDL, the user lists are stored on the device itself rather than the central active directory server. Users and groups can also be linked to department ID codes for centralised usage control. The user management information for SDL is entered either via a web browser or can also be imported from a text file.
Redundant System

uniFLOW Secure Printing (incl. MyPrintAnywhere)

Optional module for all editions of uniFLOW
(Any edition of uniFLOW includes 1 module of choice for free.)
uniFLOW MyPrintAnywhere allows users to release their print job on any device connected to the uniFLOW server. This allows flexibility to choose another device, e.g., if the desired device is blocked by somebody printing a huge documentation.

There are various configurations to suit different requirements:
1. MyPrintAnywhere Secure Printing: The user prints the documents from their PC. The server holds the print jobs. The server releases the print jobs to any MFP at which the user provides a valid identification.
2. Distributed Release Queue Management: The user prints the documents from their PC. One or more servers can hold the print jobs. This provides a secure global print job release mechanism that spans any number of servers.

Identification Methods
uniFLOW offers various ways of identification at the MFP:
- Entering a numeric code (e.g., a PIN code), or an alphanumeric code (e.g., a cost centre)
- Using a magnetic card
- Using a contactless card
- Using your fingerprint

MiCard & MiCard devices use the MFP’s USB connection, thereby removing the requirement for an additional IP address. This reduces the points of attack on the network and the security concerns of another network attached device.
uniFLOW provides the administrator with an extensive set of configuration options to allow the system to integrate with existing customer environments.
uniFLOW is also designed to be customisable. Any new authentication devices, mechanisms or systems can be supported quickly and efficiently on a project basis.

Therefore™ Redundant Storage
The functionality is standard with all editions of Therefore™, but needs to be configured (additional backup disks or backup server are not included).

Backup Disks
Documents are secured against disk corruption. If documents are stored in one place only, the disk may get corrupted and result in data loss. Even with RAID disks, it may happen that someone in an administrative function may erroneously delete a file from the Therefore™ store. Therefore™ Migrate application manages migration of data from one disk to another remote disk per schedule.
The customer benefits from assurance that their valuable data is available in more than one location, should primary disk fail.

A Backup Server is a second Therefore™ Server in a remote physical location. (Enterprise Edition required). Customers can build a Therefore™ system where all documents are automatically migrated to a second server, meaning documents are kept in two physically separated locations. With such a backup system, customers can secure their documents against disasters like fire or earthquake.

5 Key Points to Remember about Availability

- Availability means making sure that secure information is always available to those that need it.
- File encryption makes it easy for users to encrypt files, store, send and then encrypt when required.
- MyPrintAnywhere makes it easy for users to securely collect their prints at the most convenient device on the network.
- Secure Watermarks can be used so that when copied a document’s watermark becomes clearly visible.
- Canon’s Therefore™ system includes a back-up server capability enabling documents to be located in two separate physical locations.
Summary

There are numerous security measures that can secure the Confidentiality, Availability and Integrity of your business information.

Things to consider

• Did you realise that Canon has developed both standard and add-on features to suit your business needs?
Security included within Canon’s MFPs
Outlined below are the standard security features that you will find as part of the majority of Canon’s MFPs. These will provide a useful level of protection against many potential breaches. Turn to the next page to find the security capabilities that may be incorporated as “add-ons”, providing heightened security and further reassurance.

Standard Security Features

**Department IDs**
Department IDs can be enabled on the MFP. The user enters their department ID code and password and can then make a print, copy, fax or scan. Without this ID code and password, the device functionality is unavailable.

**Single Sign On**
Device security can be further enhanced using the Single Sign-On feature. This provides similar functionality to department ID codes but the user enters their network username and password and will be authenticated against active directory. This makes the management of users and access rights much easier.

**Simple Device Login**
If Active Directory is not available there is another solution called Simple Device Login (also known as SDL). When using SDL, the user lists are stored on the device itself rather than the central active directory server.

**Watermark**
Visible watermarks can be applied to the printed page via the printer driver. Visible watermarks act as a deterrent and can make the company information restrictions for that document clearly visible.

**Job Log**
The MFP contains a Job Log that is accessible via the Remote User Interface. The Job Log contains information about every print, scan, fax, etc. that a user has made. The user name may be a Department ID or it may be the name of the person, depending upon the identification method used.

**IEEE 802.1X**
This provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

**Secure Printing**
The Secure Printing functionality allows the user to set a numeric password during printing. The password must be entered at the device before the job can be printed.

**Secure Mailbox**
The Secure Mailbox functionality allows the user to print to a storage area (mailbox) on the device. The mailbox is password protected (by the user) and the user can gain access to these jobs by entering the password at the device.

**IP and Mac Address Filtering**
The IP and Mac Address Filtering allows the user to block or allow specific IP or MAC addresses. The network administrator may want only 1 print server contacting the MFP. Therefore the MFP can be setup to only allow the print servers IP or MAC address to contact it, blocking all other incoming network traffic.

**Protocol Configuration**
The Protocol Configuration allows the administrator to enable and disable the network protocols.

**SSL Certificates**
SSL Certificates are used to enable HTTPS functionality on the MFP. This allows information to be securely transferred when using either the remote user interface or MEAP applications on the MFP.
Add-on Security Features

Secure the Access
Controller access to the MFP allows organisations to keep sensitive information confidential.

Department ID, Single Sign On and Secure print are some of the standard features that provide the ability to secure access to this information but why not consider uniFLOW secure printing options.

uniFLOW Secure Printing provides users with effective security mechanisms to control the output of sensitive documents. Print jobs are held on the server and can only be retrieved at the MFP using an appropriate identification method. To allow for secure printing, user identification at the MFP is needed.

Secure the Data
Protecting the data within the MFP during the storage or transit of this information is vital in keeping sensitive information secure.

Canon offers services to help protect the data at the end of the MFD life. But why not consider utilising some of the hard drive features available during the use of the device.

The Hard Disk Encryption Kit can be added to the MFP to guarantee that the data on the hard disk will be encrypted securely. This kit is also certified by ISO 15408 (Common Criteria). Additionally, the opportunity to utilise the removable hard drive allows for the secure storage of the hard disk outside working hours.

Secure the Document
As print is a major output of the MFP, controlling the information within hard copy documents is critical.

Visible watermarking is standard on the MFP and acts as a good deterrent. But why not consider strengthening this with additional features that are available.

The document scan lock feature can embed Track & Lock code within copier printed documents to restrict unauthorised copying, sending and faxing of these documents, as well as tracking from where these documents originated.

If your business requires special or personalised document security protection, please contact Canon. Our consultants are here to help you protect your document information.

There are additional software packages that link or can be installed within our devices but are not provided as standard with the MFP.
As a key principle of privacy, the movement of personally identifiable information between entities, such as a customer list being shared between two different companies.

The opposite of encryption, decryption is the process of converting encrypted content back to its original form.

A deliberate attempt to compromise the security of a computer system or deprive others of system use.

Authentication is the process by which a person, computer process or device is validated. That is, credentials are provided to prove someone is who they say they are. Commonly this is done with usernames and password, smart cards or digital signatures.

This is the process of granting a person, computer process, or device access to certain information, services, or functionality. Authorisation is derived from the identity of the person, computer process, or device requesting access, which is verified through authentication.

The process of making secure information is readily accessible and instantly retrievable by those authorised to see it, and in the format they expect.

Access Control
Access Control is used to limit information to users, based on their identity and membership of pre-defined groups. It can be mandatory, discretionary, or role-based.

Administrative Vulnerability
Logging on to an account that has more user rights than the user requires is classed as administrative vulnerability.

A hidden entrance to a computer system that can be used to bypass the system’s security policies.

The Basel Accords, which are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision. Their purpose is to create an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face.

An encrypted file containing user or server identification information. A certificate is used to verify identity and to help establish a security-enhanced link.

The ISO/IEC 15408 certification system certifies that security functions have been reliably designed and implemented. The certification covers the entire lifecycle including production, shipment, sales, installation and service. There are seven different levels of conformity distinguished by the letters EAL.

As a key principle of privacy, the movement of personally identifiable information between entities, such as a customer list being shared between two different companies.

The opposite of encryption, decryption is the process of converting encrypted content back to its original form.

A DoS is where a user maliciously prevents a user, process or system from accessing a resource, usually a network service. Examples of DoS attacks include flooding network connections, filling disk storage, disabling ports, or removing power.

A digitally signed statement that binds the identifying information of a user, computer, or service to a public/private key pair. A digital certificate is commonly used in the process of authentication and for securing information on networks.

A specific type of DoS in which an attacker uses malicious code installed on various computers to attack a single target.

Data that binds a sender’s identity to the information being sent. A digital signature may be bundled with any message, file, or other digitally encoded information, or transmitted separately and binds the sender’s identity to the information being sent. Digital information transmitted using a digital signature cannot be changed without losing the signature. In some countries, including the European Union, digital signatures have legal significance. However, laws concerning electronic signatures do not always make clear their applicability towards cryptographic digital signatures, leaving their legal importance somewhat unspecified.

A standard for sanitization to counter data remanence. It is also known as the NIST Operating Manual (NISPOM) and is issued by the National Industrial Security Program (NISP), which is the nominal authority in the United States for managing the needs of private industry to access classified information. Canon devices do currently not comply with the DoD 5220.22-M standard.
Glossary

**Encrypted Data**
Data that has been converted from plaintext into ciphertext.

**Encryption**
The process of converting data into a coded form (ciphertext) to prevent it from being read and understood by an unauthorized party.

**EU Data Protection Directive**
A European Union (EU) law stating that personal data from EU countries can only be transferred to non-EU countries provided they can provide an acceptable level of privacy protection. An organization is obliged to inform individuals why information about them is collected, how to contact the organization with inquiries and complaints, the types of third parties to which the organization will disclose, and the options an organization provides to limit the disclosure of certain information. Proper notice and choice must be offered to allow an individual to choose to opt in or out of providing specific information the organization plans to track.

**Firewall**
A firewall provides security by segregating one part of a network from another, allowing only authorized network traffic to pass through according to traffic filtering rules.

**FTP**
File Transfer Protocol is a network protocol used to transfer data from one computer to another through a network such as the Internet.

**Health Insurance Portability and Accountability Act (HIPAA)**
A U.S. regulation that gives patients greater access to their own medical records and more control over how their personally identifiable health information is used. The regulation also addresses the obligations of healthcare providers and health plans to protect health information. In general, covered entities such as health plans, healthcare clearinghouses, and healthcare providers which conduct certain financial and administrative transactions electronically had until April 14, 2003, to comply.

**HTTP**
Hypertext Transfer Protocol is a communications protocol for the transfer of information on the Internet.

**HTTPS**
(Hypertext transport Protocol secure) HTTPS is not a separate protocol, but refers to the combination of a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL) connection. Also see SSL.

**IEE P2600**
The IEEE Standards Association (IEEE-SA) has begun work on IEEE P2600(TM), Standard for Information Technology: Hardcopy System and Device Security. This new standard will define security requirements for those who manufacture, create software for and use printers, copiers, multifunctional devices and other hardcopy devices, as well as for the computer systems that support them. It will cover many aspects of security involved in developing, selecting, installing, configuring and using these devices.

**Identification**
An action that verifies the identity of the person using a system.

**JWT**
JSON Web Token is the use of a lightweight open standard to transport information securely between parties on the internet. It is designed to be interoperable with existing APIs and is a more efficient alternative to traditional state-based solutions for maintaining context between requests and responses.

**IP**
Internet Protocol is a standard communications protocol that ensures data is delivered from its source to its destination in the Internet.

**IPsec**
IPsec protocols operate at the network layer (layer 3 of the OSI model). Other Internet security protocols, such as SSL, operate from the transport layer up (OSI layers 4 - 7). This makes IPsec more flexible, as it can be used for protecting transport layer protocols. IPsec has an advantage over SSL and other methods that operate at higher layers: an application doesn’t need to be designed to use IPsec, whereas the ability to use SSL or another higher-layer protocol must be incorporated into the design of an application.

**IPPPS**
The Secure Internet Printing Protocol allows for encrypted printing.

**Key**
A value used in combination with an algorithm for encrypting or decrypting data.

**Local Attack**
An attack that targets the computer which the attacker is logged on to.

**Malicious User**
A user who intentionally accesses a system with the specific intent of causing harm.

**Message Authentication Code (MAC)**
An algorithm that allows a receiver to ensure that a block of data has remained its integrity from the time it was sent until the time it was received.

**MEAP**
The Multifunctional Embedded Application Platform is an application development platform that allows the creation of embedded applications for Canon multifunctional peripheral devices. Custom applications can be created to execute on the device itself.
Network Log on
The process of logging on to a computer via a network.

Non-repudiation
A technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Non-repudiation provides proof that a user took a specific action such as transferring money or authorising a purchase.

Password
Used to verify identity to a network or local computer and represented by a string of characters.

Password Synchronisation
A method used to replicate passwords between multiple computers, devices, folders, or networks, in order that the same password can be used across all environments.

Permissions
Authorisation to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Identification Number (PIN)
A secret identification code similar to a password. Used to access banking systems and MFPs.

Personally Identifiable Information (PII)
Any information relating to an identifiable individual. For example, name, country, street address, e-mail address, credit card number, or IP address. Sometimes called personal data or personal information.

Physical Vulnerability
Failure to provide physical security for a computer, such as leaving an unlocked computer running where it could be used by unauthorised users.

Privacy
Privacy is defined as the control that individuals have over the collection, use, and distribution of their personal information.

Private Key
One of two keys used in public key encryption. The user keeps the private key secret and typically uses it to digitally sign data, or to decrypt data that has been encrypted with the corresponding public key.

Public Key
One of two keys in public key encryption. The user releases this key to the public, who use it to encrypt messages to be sent to the user and to verify the user’s digital signature.

Public key Encryption
An encryption method that uses a pair of mathematically related keys: a public key and a private key. Either key can be used to encrypt data, but the corresponding key must be used to decrypt it.

Public key Infrastructure (PKI)
The framework used to manage the use of public key cryptography on public networks such as the Internet.

Remote Attack
A malicious attach whereby the attacker targets a computer other than the one he is logged into.

Repudiation
The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Safeguard
A technology, policy, or procedure, policy or technology used to counter threats.

Secondary Data Uses
Uses of personal information for purposes other than those for which the information was collected.

Secure Sockets Layer (SSL)
A protocol that provides secure data communication through data encryption. It enables authentication, integrity and data privacy through a combination of digital certificates, public-key cryptography and bulk data encryption.

Sensitive Data
From the European union perspective, personally identifiable data regarding race or ethnicity, political opinions, religious or philosophical beliefs, sexual preference, or trade union membership.

Smart Card
A credit card-sized device that is used, with an access code, to enable certificate-based authentication. Smart cards securely store certificates, public and private keys, passwords, and other types of personal information.

SNTP
The (Simple) Network Time Protocol is a protocol for distributing the Coordinated Universal Time (UTC) by means of synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.

SOX
SOX regulates corporate financial records and provides penalties for their abuse. It defines the type of records that must be recorded and for how long. Affecting data storage capacities and planning, SOX was enacted after the Enron and WorldCom scandals of the early 2000s.

Strong Password
A strong password is used to create an effective defence against unauthorised access to a resource.
“Canon has delivered a secure printing network which saves us around €1 million a year”

Dr Roland Kreig, Chief Information Officer, Fraport AG, Germany

Talk to Canon’s experts about how our security solutions can protect the information of your office documents.

http://canon-europe.com/securitysolutions