Office of the Government Chief Information Officer

INFORMATION SECURITY

Practice Guide

for

Securing Network Printers

in the Offices

[ISPG-SO01]

Version: 1.0

August 2018

COPYRIGHT NOTICE

Amendment History				
Change Number	Revision Description	Pages Affected	Revision Number	Date

Table of Contents

1. Introduction

Nowadays, new generation of network printers are “smart” machines that have central processing units, the capability of storing information they processed in their internal storage devices; and connecting to wired or wireless networks. With these capabilities, most of the current network printers can be used for more than just printing; they can also be used for copying, scanning, faxing and emailing documents. Some of the network printers even have internal servers or routers. Hence, network printers are similar to other computer equipment which could be suffered from various types of security threats (e.g. data leakage) if they are not properly protected / used.

This practice guide is developed to provide guidance notes for Bureaux/Departments (B/Ds) to make reference in securing the use of network printers in their offices.

1.1 Purpose

This document provides guidance notes for the administration and other technical and operational staff who are involved in managing network printers. Common security considerations and best practices on major stages of network printer management life cycle for using network printers are provided in this document. B/Ds should consider the security measures and best practices recommended in this document and implement adequate security protection for their network printers. This document should be used in conjunction with the established government requirements and documents including Baseline IT Security Policy [S17], IT Security Guidelines [G3], relevant procedures and guidelines, where applicable. In addition to the government security requirements, B/Ds should assess the security risks before the adoption of network printers based on their business needs.

This document is intended to provide practical guidance notes on and references for management and use of network printers in the offices. It is not intended to cover technical requirements of a specific network printer model. B/Ds should consult corresponding system administrators, technical support staff and product vendors for these technical details.

1.2 Normative References

The following referenced documents are indispensable for the application of this document.

- Baseline IT Security Policy [S17], the Government of the Hong Kong Special Administrative Region
- IT Security Guidelines [G3], the Government of the Hong Kong Special Administrative Region

1.3 Terms and Convention

For the purposes of this document, the terms and convention given in S17, G3, and the following shall apply.

Abbreviation and Terms	
N/A	N/A

1.4 Contact

This document is produced and maintained by the Office of the Government Chief Information Office (OGCIO). For comments and suggestions, please send to:

Email: it_security@ogcio.gov.hk

Lotus Notes mail: IT Security Team/OGCIO/HKSARG

2. Information Security Management

Information security is about the planning, implementation and continuous enhancement of security controls and measures to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission and its associated information systems. Information security management is a set of principles relating to the functions of planning, organising, directing, controlling, and the application of these principles in harnessing physical, financial, human and informational resources efficiently and effectively to assure the safety of information assets and information systems.

Information security management involves a series of activities that require continuous monitoring and control. These activities include but not limited to the following functional areas:

- Security Management Framework and the Organisation;
- Governance, Risk Management, and Compliance;
- Security Operations;
- Security Event and Incident Management;
- Awareness Training and Capability Building; and
- Situational Awareness and Information Sharing.

Security Management Framework and Organisation

B/Ds shall establish and enforce departmental information security policies, standards, guidelines and procedures in accordance with the business needs and the government security requirements.

B/Ds shall also define the organisation structure on information security and provide clear definitions and proper assignment of security accountability and responsibility to involved parties.

Governance, Risk Management and Compliance

B/Ds shall adopt a risk based approach to identify, prioritise and address the security risks of information systems in a consistent and effective manner.

B/Ds shall perform security risk assessments for information systems and production applications periodically and when necessary so as to identify risks and consequences associated with vulnerabilities, and to provide a basis to establish a cost-effective security program and implement appropriate security protection and safeguards.

B/Ds shall also perform security audit on information systems regularly to ensure that current security measures comply with departmental information security policies, standards, and other contractual or legal requirements.

Security Operations

To protect information assets and information systems, B/Ds should implement comprehensive security measures based on their business needs, covering different technological areas in their business, and adopt the principle of "Prevent, Detect, Respond and Recover" in their daily operations.

- Preventive measures avoid or deter the occurrence of an undesirable event;
- Detective measures identify the occurrence of an undesirable event;
- Response measures refer to coordinated actions to contain damage when an undesirable event or incident occurs; and
- Recovery measures are for restoring the confidentiality, integrity and availability of information systems to their expected state.

Security Event and Incident Management

In reality, security incidents might still occur due to unforeseeable, disruptive events. In cases where security events compromise business continuity or give rise to risk of data security, B/Ds shall activate their standing incident management plan to identifying, managing, recording, and analysing security threats, attacks, or incidents in real-time. B/Ds should also prepare to communicate appropriately with relevant parties by sharing information on response for security risks to subdue distrust or unnecessary speculation. When developing an incident management plan, B/Ds should plan and prepare the right resources as well as develop the procedures to address necessary follow-up investigations.

Awareness Training and Capability Building

As information security is everyone's business, B/Ds should continuously promote information security awareness throughout the organisations and arrange training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and conform to security best practices.

Situational Awareness and Information Sharing

As cyber threat landscape is constantly changing, B/Ds should also constantly attend to current vulnerabilities information, threat alerts, and important notices disseminated by the security industry and the GovCERT.HK. The security alerts on impending and actual threats should be disseminated to and shared with those responsible colleagues within B/Ds so that timely mitigation measures could be taken.

B/Ds could make use of the cyber risk information sharing platform to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

3. Network Printer Security

In information security management, the "Security Operations" functional area includes the deployment of proper security protection and safeguards to reduce the risk of successful attacks. In light of the ever-increasing abilities of network printers which have the similar capabilities of networked computer equipment, network printers are also facing similar security threats that need to be properly managed. Network printer security is, therefore, a major area under the "Security Operations" functional area of information security management.

This section highlights the security measures and best practices to address the common security concerns and illustrates how they should be incorporated in the major stages of network printer management life cycle including provision, use and decommission. B/Ds may select and map the security measures and best practices to their own management life cycle model based on their business needs.

3.1 Security Concerns of Network Printers

Network printers have the capabilities of storing data in their storage devices and connecting to wired or wireless networks for printing, copying, scanning, faxing and emailing documents. They can also use network protocols commonly available in computer equipment, such as File Transfer Protocol (FTP), Hyper Text Transport Protocol (HTTP), Hyper Text Transport Protocol Secure (HTTPS), Internet Printing Protocol (IPP), Server Message Block (SMB), Simple Network Management Protocol (SNMP) and telnet. Hence, network printers expose similar security threats faced by other connected computing devices. Major threats applicable to network printers are highlighted below. B/Ds should take reference of these common security threats and avoid them in using network printers.

3.1.1 General Threats and Vulnerabilities

General threats, vulnerabilities, and related exploits that may affect network printers:

- **Default administrator account name and password** – Attackers easily gain access and control of network printers if default administrator account name and password is left unchanged or weak password is used.
- **Outdated and/or unpatched operating systems and firmware** – Network printers run embedded commercial operating systems which render them subject to the same threats and vulnerabilities as any other computing devices running the same operating system. Attackers may exploit vulnerabilities to gain access and control of network printers if the operating system and firmware are unpatched or outdated.
- **Lack of physical security controls** – Network printers and their built-in storage devices have the risk of lost or stolen if the printers are installed in uncontrolled places.

- **Document theft** – The printouts could be seen or taken by unintended parties.

3.1.2 Network Connectivity Threats and Vulnerabilities

Although using network printers is convenient and may be more cost-effective than using separate local printers, scanners and fax machines; network connectivity comes with greater risk of exposing the device and information to threats. Some potential threats, vulnerabilities, and related exploits associated with network connectivity include:

- **Unencrypted information** – Any information, including configuration data or passwords, sent unencrypted to network printers could be intercepted, exposed and/or altered.
- **Wireless connectivity** – Wireless networks, such as Wi-Fi network, are inherently unsafe and susceptible to eavesdropping, which place information transmitted at risk of compromise and may lead to a security breach.
- **Network protocols** – Most network printers provide services via variety of network protocols such as FTP, HTTP, IPP, SMB, SNMP and telnet. Yet each protocol has its own threats and vulnerabilities to be managed. Therefore, unused services / protocols shall be disabled to minimise the associated risks.

3.1.3 Data Storage Threats and Vulnerabilities

Data storage in network printers is most often in the form of hard disk drive (HDD) or solid-state drive (SSD). Information stored in network printers may leave organisational information vulnerable to numerous exploits and leakage in the following conditions:

- **Unencrypted information** – Any information stored unencrypted on network printers could be exposed and/or modified by anyone with access or in the event of a successful network-based attack.
- **Sanitisation** – If network printers are disposed without properly data erasure, unauthorised personnel may recover the information left inside the storage device.
- **Unauthorised access** – External maintenance or personnel with physical or remote access to network printers could download or copy the stored information.

3.2 Provision of Network Printers

When considering security adoption of network printers, B/Ds should identify the needs for network printers and how the network printers would support B/Ds' businesses. A network printer security policy should be established to specify the business and security requirements for the use of network printers with the following considerations:

- The types of approved network printers and the approval mechanism.
- The data classification permitted on each type of network printer. Classified information shall be encrypted when stored in network printers.
- The control mechanism to ensure the compliance with the government security requirements based on the data classification.
- The procedures to ensure complete erasure of government data stored in network printers when they are disposed.

Based on the business and security requirements, B/Ds should develop adequate processes and procedures for the provision of network printers. In particular, security configuration procedures of network printers should be developed to enforce security configurations in accordance with government security requirements and the network printer security policy. Network printers should be configured according to the security configuration procedures before deployment. For sample checklist regarding security configuration of a network printer, please refer to **Annex A**.

The following best practices should be included in the provisioning stage:

a. Identify the list of supported model that fulfils B/Ds' operations and security requirements.

b. Perform risk assessments prior to deployment of new network printers, and implement a continuous risk monitoring mechanism for evaluating changes in or new risks associated with the network printers.

c. Disseminate the acceptable use policy and security reminders; as well as provide security awareness trainings to users to remind them to use network printers in a secure manner.

d. Maintain asset-tracking information such as serial number and keep track of them for audit and development of B/Ds' technology replacement strategy for network printers.

e. Apply secure configuration

   - Isolate network printers from other systems until the secure configuration is completed;
   - Remove unused applications from network printers, e.g. Internet browsers;
   - Enable all applicable security features of network printers according to the

security configuration procedures of the network printers, including strong password for administrators of network printers and encryption of data stored on storage devices;

- Enable immediate file overwrite to delete temporary file of each job[1];
- Enable regular off-hours overwrite, if applicable;
- Enable pull / private printing solutions which allow setting password for a print job and users can release this print job only when the password is entered;
- Enable removal of print jobs for pull / private printing from the printer's storage devices after predefined timeout period; and
- Change default administrator account names / passwords and use strong passwords for network printers.

f. Enable network security

- Restrict network printers from accessing the Internet and configure the network printers to work within B/Ds' internal trusted networks;
- Protect printers with firewall, if available, to only allow authorised traffic from/to the printers;
- Enable HTTPS for web interface, if available, to access the printers' admin functions; and
- Enable network encryption protocols (e.g. SSL/TLS, IPsec), if available, to ensure that messages sent between computers and the printers are kept secure.

g. Limit/restrict access

- Enable identification and authentication for privileged access (e.g. change the configuration settings);
- Disable unauthorised remote access of network printers;
- Disable unneeded management services, ports and protocols;
- Disable wireless network connection for handling classified information;
- Whitelist or blacklist specific Media Access Control (MAC) addresses and/or IP addresses; and
- Implement appropriate physical security.

[1] Some printers do not support file overwrite when SSD is used as storage device. B/D could select HDD if the file overwrite feature is necessary.

3.3 Management of Network Printers

Even if the security requirements have been fully considered in the provisioning stage, people and process are two main factors for keeping network printers in a safe environment. Therefore, this section focuses on the best practices related to on-going operation process for the management of network printers whereas best practices for using network printers by end-users are provided at **Annex B**.

3.3.1 On-going Operation of Network Printers

Administrators should follow the best practices as follows:

a. Check the status of network printers regularly to ensure security measures are in place;

b. Change password for administrators of network printers regularly;

c. Review user accounts and privileges regularly to prevent unauthorised access of network printers;

d. Update the operating system / firmware regularly to patch security vulnerabilities and improve security features;

e. Make sure after any system / firmware updates or cold resets, all the established security controls are reinstated; and

f. Review the print logs regularly, if applicable, to identify any suspicious activity such as the volume of print jobs or time of printing.

3.3.2 Handling Classified Information

In compliance with the security requirements of the Government, B/Ds shall observe government security requirements and documents. In addition, B/Ds should adopt the following security practices for handling classified information:

a. Do not print/copy/scan/fax/email TOP SECRET or SECRET information with network printers.

b. Wireless network is very vulnerable and must not be used to transmit classified information without any control. If transmission of CONFIDENTIAL information to/from network printers via wireless networks is required, approval from Head of B/D must be sought for both the transmission of CONFIDENTIAL information through the wireless networks and the devices used for the transmission.

c. Encrypt all CONFIDENTIAL or RESTRICTED information when transmitted from/to or stored in network printers (e.g. printer's hard disk drive), either temporarily or permanently for printing, copying, scanning, faxing or emailing

documents. B/Ds should check with product vendors to ensure the network printers can meet the encryption requirements for handling classified documents.

d. Detailed encryption requirements for these two types of classified information are given below.

Encryption requirements on CONFIDENTIAL information

- CONFIDENTIAL information must be encrypted during storage and transmission over an un-trusted communication network, e.g. wireless network. If symmetric encryption is selected, the key length shall be at least 128-bit for the Advanced Encryption Standard (AES) encryption or equivalent. If asymmetric encryption is selected, the key length shall be at least 2048-bit for the RSA encryption. Alternatively, the requirement can be met by Elliptic Curve Cryptography (ECC) encryption with key length of at least 224-bit or equivalent.
- For keys that are used for decrypting CONFIDENTIAL information, they shall be stored separately from the corresponding encrypted information.

Encryption requirements on RESTRICTED information

- RESTRICTED information must be encrypted during storage and transmission over an un-trusted communication network, e.g. wireless network. If symmetric encryption is selected, the key length shall be at least 128-bit for the Advanced Encryption Standard (AES) encryption or equivalent. If asymmetric encryption is selected, the key length shall be at least 2048-bit for the RSA encryption. Alternatively, the requirement can be met by Elliptic Curve Cryptography (ECC) encryption with key length of at least 224-bit or equivalent.

e. If network printers with storage devices do not meet the above encryption requirements, B/Ds should consider using network printers without built-in storage device and connecting the printers to a trusted network. Alternatively, local printers without built-in storage devices may be used.

f. If classified information is stored in network printers' storage devices, the network printers shall be installed in a physically secure environment. Security measures preventing any possible interfering of the printers shall be put in place.

g. Completely clear or destroy all classified information stored in network printers when they are no longer required.

3.3.3 Awareness Training

Awareness training is an important activity to promote both administrators and users security awareness in using network printers. Awareness training to administrators should be arranged to enable them to fully understand the potential security threats encountered, the security requirements of network printers and possible security measures. For general users, trainings may be via user guide, circular or email to raise their awareness of best practices of using network printers.

Generally speaking, awareness training should include but not limited to:

a. Information classification and corresponding security requirements for handling information with network printers.
b. Protection of printouts.
c. Security requirements for network printers in provision, using and decommissioning stages.

3.4 Decommissioning of Network Printers

At the last stage of network printer management life cycle, network printers may be decommissioned due to physical damage, end of support, re-use by other staff or other B/Ds, etc. B/Ds should define device decommission procedures covering secure data deletion and network printers factory reset and disposal such that network printers can be re-used or securely disposed without data leakage.

a. Secure Data Deletion
    - Clear all the logs and data from network printers. Some network printers provide features to remove information from both non-volatile random-access memory (NVRAM) and hard drive. If no such feature, the NVRAM and hard drive should be wiped manually using data removal software solution or physical destruction.

b. Factory Reset
    - Restore network printers to default factory setting. It could be done by using the "Restore Factory Settings" function, if available. B/Ds may seek advice from the corresponding product vendors, if necessary.

All classified information stored in network printers shall be completely cleared from the storage media before disposal, re-use or repair in accordance with government security requirements. If for any reason this is not feasible, the storage media must be physically destroyed to prevent the recovery of the classified information.

*** ENDS ***

Annex A: Sample Checklist on Security Configuration for Network Printers

The following list of configuration is recommended for securing network printers used in the offices. B/Ds may adjust the checklist based on their specific business requirements and advice from product vendors or third party consultants, if applicable.

	Configurations
Preparation and Installation	
1.	Isolate the network printer from other systems until the secure configuration is installed and hardened.
2.	Install the network printer in physically secure environment.
Network Control	
3.	Disable all protocols[2] if they are not being utilised (e.g. AppleTalk, IPX/SPX).
4.	Assign the network printer with a static IP address[3] or limit network access to the printer as possible such as access control lists in the printer configuration.
5.	Use secure communications (e.g. enable HTTPS for web-based management).
6.	Encrypt network traffic (e.g. IPsec or SSL/TLS).
7.	Disable wireless network connection for handling classified information.
Data Protection Control	
8.	Encrypt data stored in the printer's storage devices, if applicable.
9.	Ensure that data stored in printer's storage devices is erased completely before decommission.
10.	If printer's storage devices are used for printing, copying, scanning, faxing or emailing documents, configure the network printer to remove any spooled files, images, and other temporary data from the storage devices using a secure overwrite between jobs.
11.	Enable authenticated retrieval of print jobs for users, e.g. pull / private printing.

[2] For examples:

i) IPP: If the Internet Printing Protocol is not used, then disable it.
ii) FTP: This feature is not used in most environments and should be disabled.
iii) SMB: Most printers do not provide status report when using SMB printing and should be disabled.

[3] Giving static IP addresses or DHCP reservations makes it easier to monitor the printers and apply access lists on hardware-based firewalls. Consider placing sensitive printers on their own subnet, which may make them easier to identify and secure.

12.	Enable Secure Multipurpose Internet Mail Extensions (S/MIME) for email transmission of documents, if applicable.
Administration Control	
13.	Disable all services not used (e.g. FAX, scanner). If the web interface is not required, consider disabling the web server.
14.	Change the default administrator account name / password, if applicable.
15.	Set strong passwords for administrator accounts according to password policy.
16.	Restrict access to management console.
17.	Disable unneeded services and management protocols[4].
18.	Apply latest patches for printer's operating system and/or firmware.
19.	Disable unused communication ports (e.g. Bluetooth, Wi-Fi, NFC, USB).
20.	Disable unauthorised remote access.
User Authentication / Authorisation Control	
21.	Enable user identification and authentication for privileged access.
22.	Restrict users to change the configuration settings.
23.	Ensure that only authorised users can modify the global configuration from the console by requiring a password.
Logging	
24.	Enable logging (e.g. access log) and review the logs regularly, if applicable.

The above checklist is NOT exhaustive and only includes some of the most common practices on printer configuration.

[4] For examples:
i) Disable web interface if possible; otherwise, enable HTTPS and disable HTTP at least.
ii) Disable telnet management interface.
iii) Disable SNMP if not used for printing management in your office; otherwise, choose SNMPv3 for its authentication and encryption features if possible.

Annex B: Use of Network Printers

Even the network printers have been prepared for secure operation, users should follow the best practices as follows:

a. Use authorised network printers.

b. Do not use printer's wireless connection functionality to handle classified information.

c. Observe the security requirements of printing, copying, scanning, faxing and emailing classified documents.

d. Use pull / private printing feature so that printouts are only released upon user authentication (e.g. PIN, smart cards) to prevent unintended disclosure of printouts containing classified information.

e. Collect the printouts as soon as possible.

f. Do not collect or copy printouts which belong to others and put them back if they are collected unintentionally.

g. Set user passwords and select strong encryption method for scanning documents, if applicable.