PolyU Multifunction Printer Standard Guidelines

Information Technology Services Office **Campus Sustainability Office**

Date of release: 31 Oct 2018

Background

Today's multifunction printer (MFP) does more than print. It scans, sends and stores potentially sensitive information. Innovations surrounding networked printers help streamline business processes and increase productivity. Printers process documents created by users and business applications across the entire University on a daily basis and some of these documents represent and contain confidential information that demands our attention. It is important to safeguard sensitive/confidential information and limit access on a need-to-know basis. Users are therefore advised to consider and implement appropriate measures and practices to ensure effective and secure printing, particularly when sourcing printing solutions to meet their operational requirements.

Secure print is a printing task that outlines a standard that all should meet for the sake of privacy and prevention of unauthorized use of printed information. Secure print deals with issues including access levels and the need to control printing according to the users who are accessing the setup. For instance, it may include mandatory PIN number input or other security measures to ensure that the user holding the digital assets can monitor the print job and protect its privacy.

Printing Security Considerations that Users should Pay Attention to:

1. Network Security Features & Standards
   Multifunction printers have hard drives and network access. They can be hacked like computers and be an entry point for malware and viruses.

2. Fleet Management
   Lack of control of printers can lead to inefficient, incomplete and time intensive efforts by IT to establish and maintain security settings on printers.

3. Document Security
   Output trays are an easy way for sensitive data to fall into the wrong hands.

4. User Authentication & Access control
   Without requiring user credentials, it is possible for sensitive documents to be retrieved by any users. Anyone who can access the printer settings can exploit permissions.

5. Printer Hard Drive Security
   Printing and imaging devices store user credentials and other sensitive data that can be accessed if it is not encrypted or periodically erased.

PolyU Printing Standards & Recommendations to Safeguard Printing Security

- Spool Printing
  All jobs must be spooled to MFP and can only be printed upon staff or student card reading/ authentication by mandatory PIN number input or other security measures, to ensure that the user can monitor the print job and protect its privacy.

- Secure Printing
  All print jobs must only be printed after user log in. No direct printing should be allowed.

- Usage Report
  All printed jobs must be logged for generation of usage reports down to user level for review by Department. Access may also be granted to the Campus Sustainability Office (CSO) for review of paper consumption.

- MFP should be physically connected to the Local Area Network (LAN).

- Static IP should be used with one fixed IP for one device.

- Secure protocols should be used for remote configuration and support (https, SSL, or SSH).

- All unused ports and services should be disabled.

- File Transfer Protocol (FTP) and Telnet services should be disabled.

- PolyU SMTP mail gateways should be used for all SMTP traffic.

Enquiry

For any enquiries, please contact the IT HelpCentre (Tel: 2766 5900, WhatsApp/WeChat: 6577 9669).