California
DEPARTMENT OF TECHNOLOGY
Office of Information Security

CYBER SECURITY TIPS

MAY 2017 (Revised)

Security Considerations for Multi-Function Devices (MFD)

A Multi-function Device (MFD) is an office machine which incorporates the functionality of multiple devices in one and generally provides centralized document management/ distribution/production in an office setting. An MFD may act as a combination of some or all of the following devices: printer, copier, scanner, fax, and e-mail. These devices are also referred as Multi Function Printer/Product/Peripheral (MFP), or a multifunctional, all-in-one (AIO). For purposes of this Information Sheet, these devices will be referred to as MFDs.

MFDs can help reduce organizational costs, support greening and environmental efforts, and increase employee productivity. There are however, security risks associated with the use of MFDs if not properly configured and secured. Some security risks include denial of service attacks and compromise of personal and confidential information. The procurement, implementation and operation of MFDs must be properly managed by both the business/program areas as well as the agency information technology (IT) organization.

Security risks must be considered and an appropriate mitigation strategy adopted and documented in the agency's risk analysis before MFDs are implemented in *either* a stand-alone or networked environment.

Implement Good Business Practices

It's important to ensure device access and user management controls are implemented and known to all employees. These controls should include well documented and publicized procedures that

identify; 1) prohibited practices related to MFDs; 2) procedures requiring business areas to justify the need for the MFD through a written authorization process prior to procuring or connecting the MFD; and 3) sufficient manufacturer technical specification reviews, configurations, and testing to support the agency security policy requirements. MFDs should **NEVER** be procured or attached to **ANY** network without the prior written authorization of the agency's IT organization and the Information Security Officer (ISO). Additional recommended practices include:

- Ensure the IT organization and the Information Security Officer (ISO) are actively involved in the copier procurement and non-standard support functions which may historically belong to the facilities staff.
- Implement an MFD security policy and incorporate the identification of risks associated with the MFDs and potential disclosure issues into the organization's annual security and privacy awareness training.

CYBER SECURITY TIPS: Security Considerations for MFD

- Ensure MFDs comply with all applicable policies, such as existing facsimile requirements or existing fax policy regarding scanning of documents associated with fax transmissions.
- Ensure any MFD that processes or stores data is in compliance with internal policies such as those related to computer operating systems, configuration management and patch management. For example, if an MFD has an underlying MS Windows™ based operating system, the MFD must comply with Windows™ policies and receive regular (hardware and software) maintenance.
- Prohibit the scanning of documents containing confidential or sensitive information for email transmission that leaves the secure network.
- Ensure all email transmissions from an MFD comply with existing email policies and practices, including:
  - Limit outbound MFD email transactions to sending a scanned document to single email address, specifically prohibiting large group distribution.
  - Prohibit broadcast emails concurrently with inbound or outbound faxes or scanned documents.
- Purchase the MFD with a clause that allows the agency to maintain physical custody of the hard drive when repair is required or at end of life. Before transfer and disposition of the MFD, take active measures to securely sanitize or destroy its hard drive and require the hard drive be swapped or returned during a service call.

Configure the MFD Correctly

Before installing an MFD, review the manufacturer's guidelines, the National Institute of Standards and Technology (NIST) National Checklist Program, and the Department of Defense's MFD and Printer Checklist for guidance in properly configuring the security features. See the Resources section of this Information Sheet for access to these publications online. The following is additional MFD configuration guidance:

- Delete any software applications from the MFD that are not required or approved for the operation of the MFD.
- Ensure the MFD is flash upgradeable and is configured to use the most current firmware available.
- Disable all unneeded management protocols and services (i.e., DHCP, SMTP, and BOOTP).
- Ensure any default passwords are replaced with complex passwords.
- Disable dial-in diagnostic capabilities.
- Disable Internet processing through the MFD.
- Ensure the MFD can be remotely managed **ONLY** by authorized IT administrator personnel from specific (non-publicized) Internet Protocol (IP) addresses.
- Configure the MFD to prevent unauthorized IT administrator personnel from altering the global configuration of the MFD.
- Consider disabling the re-print feature or at a minimum, provide training to employees to make them aware of inappropriate use of the re-print feature.
- Ensure the MFD maintains its configuration state (passwords, service settings, etc.) after a power down or reboot occurs.
- Establish physical security for any MFD that has removable hard drives.
- Verify that the MFD has a mechanism to lock and prevent unauthorized access to the hard drive. Keep the keys in a secure location.
- For MFDs where print spoolers are used:
  - To prevent denial of service, verify that the MFD is configured to restrict jobs to only print spoolers and cannot directly accept one or more large print jobs from unauthorized users. If supported, implement IP address restrictions. If not supported, consider placing the MFD behind a firewall, switch or router with an appropriate discretionary access control (DAC) list.

  - Configure the print spoolers to restrict access to authorized users and restrict users to managing their own individual jobs.
  - Configure MFDs and their spoolers to have auditing fully enabled.
- Identify all staff with access to the data stored on the MFD (in the event of a security incident and/or privacy breach).

Configure the Network Appropriately

Because these devices are typically connected to an organization's network infrastructure, there can be increased security and privacy risks. An important risk mitigation strategy for MFDs is to also ensure the internal network is configured properly. The following is network configuration guidance for MFD implementations:

- Isolate the MFD on the local area network, utilizing Virtual Local Area network (VLAN), switches, or router controls.
- Assign each MFD a static IP address so that if the Domain Name System (DNS) cache is poisoned (corrupted), print files containing sensitive data cannot be redirected, leading to the further compromise of sensitive data.
- Ensure that a firewall or route rule is established to block all ingress and egress traffic from the enclave perimeter to the MFD.

Establishing a defense in depth approach, such as the security considerations discussed above, will help ensure MFDs are used in a secure manner within the office environment.

Resources

- Internal Revenue Services - *Publication 1075, Tax Information Security Guidelines For Federal, State And Local Agencies* - http://www.irs.ustreas.gov/pub/irs-pdf/p1075.pdf
- NIST National Checklist Program - https://www.nist.gov/programs-projects/national-checklist-program
- NIST *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers* (SP 800-70) - http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf
- Department of Defense *Multi-Function Device and Network Printers STIG Version 2, Release 9 Checklist Details* https://nvd.nist.gov/ncp/checklist/371 and *Sharing Peripherals Across the Network (SPAN) STIG Version 2, Release 4. Checklist Details* - https://nvd.nist.gov/ncp/checklist/459
- NIST *Guidelines for Media Sanitization* (SP 800-88) - http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819
- University of Maine at Fort Kent, *Your Password, Your Identity, Your Privacy* - https://engineering.purdue.edu/people/george.a.bailey.1/Awareness/presentations/password_basics.pdf

California Department of Technology
Office of Information Security

For more cyber security tips, visit the OIS website:
https://cdt.ca.gov/security/