

## **Multifunction Device Best Practice**

This document outlines the University of Tennessee best practices for securing Multifunction Devices.

### **OVERVIEW**

This document outlines the University of Tennessee best practices for Multifunction Devices (MFD). A MFD is an office machine such as a copier or printer that combines two or more functions (such as printing, scanning, emailing, faxing, copying, storage of documents, etc.) into a single, consolidated system. Through the configuration and procedural practices outlined in this best practice, MFDs can be protected to minimize the risk of unauthorized exposure or modification of information, and to aide in ensuring the availability of those resources. All users and system managers are responsible for taking the appropriate steps, as outlined below, to secure their Multifunction Devices.

This best practice applies to all students, faculty, staff, and others, referred to as “users” throughout this best practice, while accessing, using, or handling the university’s IT resources. In this best practice, “users” includes but is not limited to subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities that are granted access as defined in the *Acceptable User of Information Technology Resources Policy (IT0110)*.

### ***Information and System Classification***

University faculty, staff, students, and others have a business need to collect, transmit, store, or process information. Protecting the confidentiality, integrity, and availability of this information is the responsibility of the entire university.

The *Information Classification Policy (IT0115)* and *Computer System Classification Policy (IT0116)* formalize this responsibility, define a framework for categorizing information and computer systems according to the perceived risk to the university, and provide a methodology for implementing these practices. Refer to those policies for definitions of ownership, responsibilities, system classifications, and information classifications mentioned hereafter.

University policies mentioned in this document can be found from the *University of Tennessee System Policy Search Page* at “<http://www.tennessee.edu/policy/>”. Best practice documents are referenced from the *Information Security Office* home page at “<http://security.tennessee.edu/>”.

## ***Compliance***

Any non-compliance with the university's Information Technology Security Strategy, policies, or best practices must be reported to the ISO. Non-compliance can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action. Reference the *Information Technology Acceptable Use of Information Technology Resources Policy (IT0110)* for information concerning non-compliance issues.

## ***Exceptions***

Compliance with the university's Information Technology Security Strategy, policies, and best practices are mandatory. In some instances, exceptions to policies and best practices must be made due to extenuating circumstances. Such exceptions must be documented and approved prior to implementation. The process for reviewing and approving/disapproving requests for exceptions can be found at (<http://security.tennessee.edu/>).

## **REQUIREMENTS AND RECOMMENDATIONS**

The security requirements and recommendations for MFDs are divided into multiple sections according to the information and system classifications of the device. The information and system classification levels determine whether the guidelines are required, recommended, or optional. In the absence of other factors, it is preferred that all devices be configured with the most secure options available.

### ***Procedural Requirements for All Multifunction Devices***

1. All MFDs must be registered with the POA or their designee. At a minimum, the following information is required and must be maintained to provide accurate identification:
  - Primary point of contact(s), a backup contact, and the physical location
  - Identification of Information Manager, Information Custodian, and Information Classification according to Policy IT0115.
  - Identification of System Manager, System Custodian, and System Classification according to Policy IT0116
  - Hardware make, model, and manufacturer
  - Main functions and any associated applications
  - All associated IP Addresses and IP names
  - All associated wired and wireless MAC addresses
2. Users and managers of a MFD must be informed of its information and system classification and must comply with the requirements for maintaining the MFD's classification.
3. All MFD managers must sign an acknowledgement form obtained from the POA or their designee that validates their understanding of and compliance with university information technology policies and best practices. The POA must maintain this signed documentation on file.

4. Passwords and passphrases must meet the complexity requirements and change frequency as defined by the *Password Best Practice* for all accounts and services on the device.
5. All individual employee accounts, pin numbers, or codes must be disabled on termination or loss of affiliation unless a college, school, or department provides documented approval and sponsorship. Also, where possible, all default account names, pins, and codes must be changed, disabled, or removed.
6. User and super-user accounts must not be shared. Accounts or individual identification (such as a pin number or code) must be uniquely assigned and separately auditable. A user account and identification assignment process must be established and approved by the POA or their designee.
7. Devices and their associated storage that are to be decommissioned or transferred must have all storage media securely erased according to the *Media Sanitization Best Practice*.
8. The appropriate Incident Response Plan must be followed in cases where there is suspicion that a device has been compromised. See the *Incident Response Best Practice* for further guidance.
9. All availability controls and processes (e.g. uninterruptible power supplies, backup and restore processes, etc.) must be tested to ensure correct operation in case of a failure.

### ***Configuration Requirements for All Multifunction Devices***

10. MFDs should have a static IP address assigned.
11. MFDs must have access controls in place to limit network traffic to the minimum communication channels that are necessary.
12. All protocols for management and operation must use standard ports, which allows for effective monitoring and control by security devices or applications.
13. Where possible, all MFDs should only accept connections from an authenticated account or system.
14. Unneeded or unused software applications or services must be disabled or removed.
15. To take advantage of improvements in security technology, MFDs must have the most current, supportable version of the firmware, operating system, and application installed that will meet the needs of the user community.
16. All firmware, operating system, service, and application security software updates must be applied as soon as possible after they become available.
17. The standard security principle of least privileged access must be used when performing an operation. For a particular process, application, or program, a user must only be able to access the minimum information and resources that are immediately necessary.
18. Access for network-based administration must be limited to encrypted methods, and to the fewest individuals and methods necessary for managing the device.

19. Restricted information (including account authentication information such as passwords) must always be transmitted over encrypted channels and must never be stored in an unencrypted manner.
20. Algorithms and protocols that make use of encryption must use standard, well-reviewed, and non-proprietary encryptions methods. (e.g., AES, Triple DES, DES-X, Blowfish, etc.)

### ***Information Protection Issues***

21. If a MFD processes or is expected to process information classified as **Confidential** or **Highly Confidential**, the system custodian must contact the ISO for additional guidance on how the MFD must be secured.
22. A MFD with hard disk storage and disk clearing capabilities must be configured to clear the disk between jobs.
  - **Public:** Clearing the disk between jobs is recommended but optional.
  - **Proprietary:** Clearing the disk between jobs is recommended but optional.
  - **Confidential:** Clearing the disk between jobs is required.
  - **Highly Confidential:** Contact the ISO for guidance.
23. The hard disk drives within a MFD should possess a mechanism to lock and prevent access to the hard drive.
  - **Public:** The use of a locking mechanism is recommended but optional.
  - **Proprietary:** The use of a locking mechanism is recommended but optional.
  - **Confidential:** The use of a locking mechanism is recommended.
  - **Highly Confidential:** Contact the ISO for guidance.
24. Physical and logical access controls (such as firewall rules, file permissions, lock and key distribution, user accounts, etc.) must adhere to the principle of least privilege, ensuring that access is granted to the fewest individuals, by the fewest methods, and in a secure manner. All controls must be reviewed periodically to ensure continued accuracy. Stale or unused permissions must be removed.
  - **Public:** The information custodian and managers must set the schedule for regular or periodic reviews mentioned above.
  - **Proprietary:** The POA or their designee must set the schedule for regular or periodic reviews mentioned above.
  - **Confidential:** The ISO must set the schedule for regular or periodic reviews mentioned above.
  - **Highly Confidential:** Contact the ISO for guidance.
25. Access control lists (such as on a router, switch, or firewall) must be used to limit inappropriate or unauthorized access from outside an academic area, business unit, or a set of specifically authorized computers. For further guidance on how network based access controls can be used to protect MFDs, consult the *Network Infrastructure Best Practice*.

- **Public:** Use of access control lists is recommended but optional.
  - **Proprietary** and **Confidential:** Use of access control lists is required.
  - **Highly Confidential:** These MFDs may not be connected to any public network. Contact the ISO for guidance.
26. Periodic assessments of the MFD and related components must be performed to ensure the MFD meets the guidelines within this best practice.
- **Public** and **Proprietary:** Security assessments at the initial installation and following each major reconfiguration are recommended but optional.
  - **Confidential:** Security assessments are required following initial configuration, following each major reconfiguration, and as part of a periodic assessment.
  - **Highly Confidential:** Contact the ISO for guidance.
27. Event logs for access controls, event monitoring, and protection hardware and software (such as firewalls, intrusion detection systems) must be monitored for suspicious activity on a regular and timely basis.
- **Public** and **Proprietary:** Periodic reviews of event logs and reports are recommended but optional.
  - **Confidential:** Event logs must be monitored on a regular basis, and reviewed for events that occur during and after work hours.
  - **Highly Confidential:** Contact the ISO for guidance.
28. Multifunction Devices may have the ability to connect to both a wired or wireless network.
- **Public:** May be connected to either a wired or wireless network. Wired network connectivity is recommended.
  - **Proprietary** and **Confidential:** May be connected to either a wired or wireless network. However, a risk assessment must be completed prior to connecting a MFD to the wireless network.
  - **Highly Confidential:** These MFDs may not be connected to any public network. Contact the ISO for guidance.
29. Where technically feasible, all unencrypted protocols must be replaced by encrypted protocols (for example scan to email and file sharing) to improve overall security. For those services that require the use of unencrypted protocols, other compensating controls must be applied to secure those communications. Appropriate documentation must be completed for any exceptions.
- **Public:** Use of encrypted protocols are optional.
  - **Proprietary** and **Confidential:** Use of encrypted protocols is required when transporting **Proprietary** or **Confidential** information.
  - **Highly Confidential:** Use of encrypted protocols is required. Contact the ISO for guidance.

30. For MFDs that lack of an appropriate level of security features supporting email functions (such as scan to email), the use of email on MFDs must be disabled.
- **Public:** Use of email is optional.
  - **Proprietary** and **Confidential:** The transmission of Proprietary or Confidential information through email is prohibited.
  - **Highly Confidential:** Contact the ISO for guidance.

### ***System Classification Issues***

31. Uninterruptible power supplies must be used to protect the device from electrical power variations that can cause outage or equipment damage. In all cases, surge protection is required to avoid equipment damage.
- **Non-Critical:** Use of uninterruptible power supplies is optional.
  - **Critical:** Uninterruptible power supplies should be used to maintain quality electrical power to devices in case of short-term variations, but is optional.
  - **Highly Critical:** Uninterruptible power supplies must be used to maintain quality electrical power to devices in case of long-term variations.
32. Production and maintenance hours must be scheduled, documented, approved, and respected. Every effort must be made to avoid outages during production hours.
- **Non-Critical:** Scheduling of production and maintenance hours is optional.
  - **Critical:** and **Highly Critical:** Scheduling of production and maintenance hours is required. The custodian and manager should approve schedules.
33. Support contracts with the appropriate vendors must be maintained to ensure expedient support in case of failure.
- **Non-Critical:** Contracts for support during production hours are optional, but recommended.
  - **Critical:** Contracts for support during production hours are required. Fast response (e.g. “four-hour turn around” or similar) and 24-hour, 7-day support is recommended.
  - **Highly Critical:** Contracts for 24-hour, 7-day, fast response support are required. Storage of spare components on-site is recommended.
34. Personnel must be available to address failures during documented production hours. Pagers and on-call lists must be used and distributed to ensure personnel are reachable. Personnel must make every effort to ensure that they are available while “on-call.”
- **Non-Critical:** Pagers and on-call lists are optional.
  - **Critical:** Pagers and on-call lists are required for production hours and recommended for non-production hours.

- **Highly Critical:** Pagers and on-call lists are required for production hours and recommended for non-production hours. Multiple persons must be available to cover production hours in case one is unreachable.

### ***Requirements for Externally-Managed Services***

Outsourced services that provide support for MFDs must follow the *Information Classification* and *System Classification* policies, even if the data resides on hardware that is not owned by the university.

Refer to the *Procurement Best Practice* for complete requirements.

35. All MFDs that store, process, or transmit the university's information must be in compliance with all appropriate University of Tennessee information technology policies and best practices.
36. There must be appropriate written contractual agreements in place to ensure service levels and compliance with applicable regulatory requirements (e.g. HIPAA, FERPA, Tennessee Code Annotated §47-18-2107, etc.).
37. There must be a clear definition of information retention and sanitization requirements as per the *Media Sanitization Best Practice*.
38. There must be a schedule for regular security assessments by the ISO or an unbiased third party. The vendor is required to take corrective action for findings identified within a contractually specified time. Results must be reported to the university.

### ***Multifunction Device Best Practice Matrix***

Numbers in this table refer to item numbers mentioned in the *Multifunction Device Best Practice*. In cases where an item has notations of “optional, with recommendations” or “required, with recommendations,” the more restrictive requirement is listed.

	<b>Optional</b>	<b>Recommended</b>	<b>Required</b>
<b>All MFDs:</b>			
Procedural			1-9
Configuration			10-20
Externally Managed Services			35-38
<b>Information Classification</b>			
<b>Public</b>	22,23,25,26 ,27,29,30	28	24
<b>Proprietary</b>	22,23,26,27		24, 25,28,29,30
<b>Confidential</b>		23	22,25,26, 27,28,30
<b>Highly Confidential</b>	Contact ISO for guidance.		
<b>System Classification</b>			
<b>Non-Critical</b>	31,32,33,34		
<b>Critical</b>		31,34	32,33
<b>Highly Critical</b>			31,32,33,34