UNIVERSITY OF CENTRAL FLORIDA

University Standards

Subject:	Multi-Function Device Standards
Standards Number:	101
Effective Date:	07-24-2010
Revised Date:	06-27-2018
Responsible Authority:	Information Security Office
Pages:	6

ACCOUNTABILITY/APPLICABILITY:

This standard applies to all multi-function devices and appliances owned by the University of Central Florida that are physically and logically capable of supporting the standard.

STANDARDS STATEMENT:

All who have access to use a networked university Multi-Function Devices (MFD) have the responsibility to ensure the overall security of the data and documents it processes. Members of the university using or administering MFDs should comply with the Data Classification and Protection policy (4-008) and the standards set forth in this document.

BACKGROUND:

The University of Central Florida has a need to centralize network capable MFDs throughout the campus to reduce the need for multiple devices, realize cost savings, simplify administration, lessen our impact on the environment, and improve process efficiencies. MFDs provide great value to the university, but also raise security concerns when not properly configured or maintained. Securing networked devices is important for a number of reasons:

- Most are simply "plugged-in" to the network using the minimal settings required for the device to operate.
- Once installed, they rarely receive security updates or patches.
- Administration of MFDs takes place on the network; physical access to the device may not be required.
- Due to increased sophistication and ever-increasing storage capacity, hackers use MFDs to launch attacks, store unauthorized data, retrieve scanned and printed documents, and print unauthorized material.

This Information Security Office (ISO) sets the minimum acceptable security standards required for attaching and deploying any MFD to the UCF network while providing for maximum security, efficiency, availability, and risk reduction.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476

STANDARDS:

1. **Passwords**
   - Follow all user and server level password standards outlined in Standards Document 501 *Password Standards*.

2. **Network**
   - Ensure embedded management web interfaces use encryption (e.g., SSL/TLS certificate issued by a trusted certificate authority).
   - Protect the embedded management web interface with a username and password.
   - Change default SNMP community strings and use SNMPv3 if possible.
   - Ensure the device can only access the internal network and not the external internet (place devices on a non-NATed VLAN.)
   - To effectively synchronize time, set the NTP servers to the following:
     - UCF Time Servers:
       - time.ucf.edu (Primary)
       - time2.ucf.edu (Secondary)
   - Disable all unused wireless communication technologies (e.g., Wi-Fi, Bluetooth, infrared, etc.)
   - If transmitting restricted data (refer to the Data Classification Policy 4-008), use only secure methods such as SMTP, SSL/TLS, SFTP, or SSH. E-mail (SMTP) should not be transmitted over plaintext channels such as FTP, HTTP, or Telnet.
     - UCF campus wide SMTP server information:
       - Configure SSL/TLS to accept all certificates without a Certificate Authority.
       - Use TLS
       - SMTP Server Address: ucfsmtps1.mail.ucf.edu
       - No authentication
       - Port: 25
       - Device must use a 10.x.x.x address to utilize SMTP
   - Disable services, applications, and user accounts that are not being utilized.
   - For the purposes of authentication to network resources such as connections to file shares for scan to file, multi-function devices must support industry standard protocols with no known vulnerabilities. Outdated, insecure protocols, such as but not limited to: SSLv2, SSLv3, SMBv1, NTLMv1, DES, etc. are not acceptable and these connections may be denied at the destination (server, file share, etc.) in order to protect UCF credentials and data.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

3. **Device Data Settings**
   - Whenever possible, disable the "save documents, copies, or scans to local device drive" (sometimes called "e-file") settings on the device. **NOTE***: Make every effort not to store data on the local MFD regardless of the selected function.*
   - Whenever possible, set device to delete documents, spooled files, images, and other temporary data using secure overwrite between jobs.
   - Whenever possible, set the device to mask the file names sent to it for processing.
   - Use encryption methods to protect data on the drive.
   - When the MFD requires maintenance or the college and/or department intends to discard the unit, always cleanse/degauss the magnetic media.
     - Always erase and over write all documents.
     - Always erase any address books on the device.
     - Use software to wipe the drive such as:
       - Active@ Kill Disk
       - Darik's Boot and Nuke ("DBAN")
       - Eraser
       - Wipe

   Note*: If the college and/or department is a customer of UCF Business Services, they have the option to use the "Toshiba Data Overwrite Kit" Contact UCF Business Services for more information:* https://copiers.busserv.ucf.edu/

4. **Logs**
   - Enable detailed system logging.
   - Review audit logs on a regular basis.
   - All devices must follow the State of Florida Records Retention Schedule.

5. **Physical Security**
   - MFD should be physically located in an access-controlled environment.
   - Disable users' ability to modify any global configuration settings.

6. **Security Awareness**
   - Educate employees and students about the risk of making copies off-site and provide information regarding the university's data policies (refer to the Data Classification Policy 4-008). This is a great opportunity to reinforce the need to protect PII.
   - Encourage users and employees to follow proper cross-shredding disposal procedures for all hard-copy documents while adhering to the State of Florida Records Retention Schedule.
   - Notify the Security Incident Response Team (SIRT) of any incidents that arise. *Contact information provided below.*

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

DEFINITIONS:

Audit log: A record that shows the identifier, date, and time that stored data is accessed.

Cross shredding: The process of using a shredder to cut paper both vertically and horizontally to more completely destroy documents.

Data: Numerical or other information represented either in a physical form or in a form suitable for electronic processing or storage.

Degaussing: The process of completely removing information from electronic magnetic media (such as traditional hard drives) so that retrieving the data is impossible.

Employees: Individuals acting on behalf of the university in processing, storing, and retrieving data. This includes any paid or volunteer acting on behalf of the university.

Encrypted or truncated: Data converted to a code or shortened for security purposes to protect its confidentiality and limit access to authorized personnel.

Information Security Office (ISO): The mission of the Information Security Office is to provide a secure infrastructure that protects the confidentiality, integrity, and availability of information resources. To this end, the ISO develops security best practices, coordinates security issues, conducts investigations, and works with Information Technology (IT) and other campus departments to minimize security risks and assure compliance with security policies and procedures.

Multi-function device (MFD): An office machine that incorporates the functionality of multiple devices in one to provide centralized document management, distribution, or production in an office setting. A typical MFD may act as a combination of some or all of the following devices: printer, scanner, photocopier, email, or fax.

Network address translation (NAT): A routing technology used by firewalls to hide internal system addresses from an external network through the use of an addressing schema.

Network time protocol (NTP): A protocol that allows other servers to download and synchronize to the official network time.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

Personal restricted data: Also called Personally Identifiable Information or PII, personal restricted data includes personally identifiable information. This is any information from which an individual may be uniquely and reliably identified or contacted (e.g., social security number, account relationships, account numbers, account balances, account histories, and passwords).

Virtual LAN (VLAN): A group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN but reconfiguring the network is accomplished through software instead of physically relocating devices.

RELATED DOCUMENTS:

2.100.1 *Florida Public Records Act—Scope and Compliance* policy
4-008 *Data Classification and Protection* policy
501 Password Standards

CONTACTS:

Information Security Office https://infosec.ucf.edu infosec@ucf.edu	Security Incident Response Team (SIRT) https://infosec.ucf.edu/incident-response/ sirt@ucf.edu
Identity Access Management (IAM) https://infosec.ucf.edu/iam iam@ucf.edu	UCF IT Support Center (407) 823-5117 https://ucf.service-now.com/ucfit itsupport@ucf.edu

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

Revision Date	Summary of Change
06-27-18	• Modified the listed UCF Time Servers • Removed broken links referenced under drive wiping software • Added statement to address the use of outdated insecure protocols

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL

(For use by the Information Security Office)

Standards Number: 101

Initiating Office: Information Security Office

Chief Information Security Officer: *Chris Vakhordjian*

Signature: chrisv Digitally signed by chrisv Date: 2019.03.18 10:03:18 -04'00' Date: 3/18/2019

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution