Standards for Utilization of Multi-function Devices	Standard No.	ITS-2013-S	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	5-2-12	Effective:	5-2-12
	Page 1 of 10			

Table of Contents

1 Purpose

The University utilizes multi-function devices (MFDs) throughout the campus as a way of reducing the need for numerous devices. A single MFD can perform multiple functions such as printing, copying, scanning, faxing and e-mail. These devices can result in reduced costs and increased employee productivity. However, these devices are actually computers, complete with operating systems, network connections and hard drive storage. This presents security risks if the MFDs are not properly configured and secured. Possible risks include:

- Loss of Level1 or Level 2 confidential data.
- Information leakage from logs (e.g., fax numbers, long distance telephone codes and filenames) that can be used for fraudulent or illegal activities.
- Simple Network Management Protocol (SNMP) attacks.
- Poorly configured network services and buffer overflows.
- Data vulnerability because physical access to the device is available to anyone, including equipment service technicians.
- Internal hard drives containing University protected data that are not data sanitized before equipment relocation or replacement.

This document sets the minimum acceptable security standards that are required for any MFD located on campus. It has been developed to secure the University and its protected data while also providing for maximum efficiency.

2 Entities Affected by this Standard

Third-party service providers are responsible for meeting or exceeding the relevant security standards when installing or servicing their equipment. Third-party service providers may not remove equipment, hard drives or any data storage components prior to data sanitization occurring.

The Procurement and Contracts office is responsible for ensuring that purchase requisitions and contracts for MFD installation and maintenance incorporate all appropriate security measures outlined herein, as well as standard information security contract language.

Departments evaluating and procuring MFDs are responsible for contacting IT Security and Compliance during the product evaluation phase to ensure these standards can be met by bidding vendors and during the vendor evaluation phase to ensure successful bidders are compliant.

Department administrators are responsible for ensuring that proper departmental information security practices are followed.

Information Technology Consultants are responsible for keeping IT Infrastructure Services informed of any network connection requirements for MFDs located within their respective academic, administrative or auxiliary units. They are also responsible for ensuring that network equipment and connectivity in their respective units meet campus standards and guidelines.

Departments responsible for any procurement, lease, rental, installation, maintenance, relocation, replacement or removal of multi-function devices must ensure that hard drive data sanitization occurs prior to equipment relocation, maintenance involving hard drive replacement/removal or equipment removal. Departments should provide sufficient notice to their designated Information Technology Consultants so they can arrange for data sanitization prior to the relocation or removal of equipment.

3 Definitions

a) Authentication: The process of confirming that a known individual is correctly associated with a given electronic credential (e.g., by use of passwords to confirm correct association with a user or account name). It is a term that is also used to verify the identity of network nodes, programs or messages.

b) File Transfer Protocol (FTP): A software standard for transferring computer files between machines with widely different operating systems.

c) Firmware: Computer programming instructions that are stored in a read-only memory unit rather than being implemented through software.

d) Internet Protocol Address: A numerical label assigned to computer network devices that uses the Internet Protocol for communication between its nodes.

e) Level 1 Confidential Data: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU’s reputation and legal action could occur if data is lost, stolen, unlawfully shared, or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a “business need-to-know.” Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information.

f) Level 2 Internal Use Data: Internal use information is data that must be protected due to proprietary, ethical, or privacy considerations. Although not specifically protected by statute, regulations or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the CSU’s reputation, violate an individual’s privacy rights or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

g) Multi-function Device (MFD): An office machine which incorporates the functionality of multiple devices in one and generally provides centralized document management/distribution/ production. A MFD is sometimes called a multifunction printer (MFP), all-in-one (AIO) device and network printer. A MFD may act as a combination of some or all of the following devices: printer, copier, scanner, fax and e-mail.

h) Protected Data: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance, or medical information. See Level 1 Confidential Data and Level 2 Internal Use Data.

i) Pull Printing: A printer feature where a user presses "print" but the document is sent to a print server or to the printer's memory instead of being printed immediately. The document is not printed until the user authentication occurs at a multi-function device (MFD).

j) Simple Network Management Protocol (SNMP): A network protocol used to manage TCP/IP networks and can be used to audit network usage, configure remote devices, detect network faults and non-authorized access and monitor network performance.

k) Social Engineering: The art of using trickery or deception to manipulate individuals into divulging confidential or personal information.

4 MFD Risks

Unsecured MFDs can disclose important information to unauthorized individuals who in turn can use this information to commit fraud, gather additional information through social engineering or obtain access to confidential documents. Following is just a sampling of the methods whereby information can be obtained. Implementing the standards in Section 5 will mitigate these risks.

4.1 Print Spool, Fax and Copy Logs

Print logs can expose network user names (e.g., JSmith32), sensitive document names (e.g., 2011_budget_details) and URLs of websites that users have printed from (e.g., https://www.myinvestments.com). Fax logs can expose incoming and outgoing fax numbers, which tell with whom you are doing business, and long distance codes and long distance credit card numbers, which may show up with the dialed numbers. Copy or scan logs contain e-mail addresses of recipients, host, user name and password information for FTP file uploads.

This information in the wrong hands enables an attacker to use social engineering to obtain further personal information, gives the attacker a picture of an individual's daily job (what they do, with whom they communicate and how to get in touch with them) and can lead to unauthorized use of long distance codes and long distance credit cards.

4.2 Lack of Physical Security

Unauthorized access to an MFD can allow malicious modifications to the global configuration from the console interface. Resetting the device back to factory defaults and then re-entering only the minimum configuration will erase any security hardening in place. Individuals can also send unauthorized faxes, obtain printouts or faxes that do not belong to them or view documents containing confidential information. Unsecured MFD locations also pose a risk from the physical removal of the hard drive, which might contain print spool files and other information.

4.3 Hard Drive Maintenance or Replacement

MFD maintenance may require that the device (including its hard drive) be returned to the manufacturer or be replaced onsite by the vendor technician. In either case, there is a risk that the original device or hard drive is not returned. This potentially exposes job spool files and other sensitive data. This same risk applies when the MFD reaches its end-of-use or end-of-lease and is returned to the manufacturer or sold.

5 Standards

MFDs use hard drives to facilitate advanced functionality. The default setting on these devices may lead to additional risk as protected data may be unknowingly stored on these devices. Security settings must be turned on or, in some cases, additional options or modules must be purchased. These devices, if connected to the campus network, should be treated like any other computer on the network.

5.1 Inventory MFDs

Document the location and related information of MFDs. Securing devices is only possible when you know how many you have, who is using them, if and where they are attached to the network and their security status.

5.2 Secure the Multi-functional Device

Make sure every MFD is protected against unauthorized access, the network and device are configured appropriately, and users are authenticated in a manner that protects University data.

5.2.1 Physical Security

Physical security is of concern when it comes to MFDs. If someone has physical access to the device any number of activities can be performed. The following standards should be met:

- Restrict who has physical access to the device. If the device regularly prints or faxes protected data, consider limiting who has access to the device by placing it in a locked room or a restricted office area to ensure that unauthorized faxes cannot be sent or obtained.
- Ensure the MFD maintains its configuration state (passwords, service settings, etc.) after a power down or reboot occurs.
- Verify that the MFD has a mechanism to lock and prevent unauthorized access to the hard drive. Keep the keys in a secure location.
- Identify all staff with access to the data stored on the MFD (in the event of a security incident or privacy breach).
- Change the initial device password from the factory default. In addition, change the device password every time it is given to a vendor service technician to perform routine or remedial maintenance.

5.2.2 Configure the Network Appropriately

If the MFD is connected to the network, the following standards should be followed:

- 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 if the Domain Name System (DNS) cache is corrupted, the print files containing protected data cannot be redirected.
- Ensure that a firewall or route rule is established to block all ingress and egress traffic from the enclave perimeter to the MFD.
- Restrict printing/copying/faxing/scanning to the minimum number of subnets practical for the device to function for its groups of users.
- Require password authentication for access to any network resources.

- Encrypt passwords when stored or transmitted over the network.
- Disable any unused ports.
- Most MFDs include an embedded web server, where http or HTTPS will likely be the primary management protocol for the device. If the MFD does not require remote management, this interface can be disabled. At the very least, see if HTTPS is supported and if http can be disabled.
- Ensure only authorized IT administrator personnel from specific (non-publicized) Internet Protocol (IP) addresses can remotely manage the MFD.
- Change SNMP community strings. SNMP community strings (similar to passwords) are often set by default to “public” for read-only access and “private” for read-write access. Many organizations do not change these. An attacker could use SNMP to gather configuration information about the MFDs or possibly modify the configuration.

5.2.3 Configure the MFD Correctly

- MFDs often come with a wide variety of services enabled, including management protocols and services. Determine if the service is needed and the risk it presents if it is used, and decide whether or not the risk is acceptable. If the risk is not acceptable and the MFD allows for it, then disable them. Chances are that many of these services are not required in all environments and should be turned off to decrease the attack footprint.
- Delete any software applications from the MFD that are not required or approved for the operation of the MFD.
- Ensure all default passwords are replaced with passwords meeting CSULA requirements.
- 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.
    - Configure the print spoolers to restrict access to authorized users and restrict users to managing their own individual jobs.
- If protected data is scanned, processed or stored on the MFD, it must have encryption and image overwrite capabilities.
- Ensure that only authorized administrators can modify the global configuration by requiring a password that is changed regularly. This will limit who can make changes (accidental or deliberate) to the global configuration.
- All MFDs should maintain current patch levels to minimize vulnerabilities. To do this it is necessary to know that security issues exist and that new firmware is available. However, MFD upgrades do not typically have an auto-update capability and are often manual processes. Information Technology Consultants should:
    - Regularly review vendor security bulletins.
    - If available, sign up for e-mails for security notification from the vendor.
    - Sign up for e-mails for security notifications from electronic mailing lists dedicated to issues about computer security.
- Revisit the requirements of the device as often as necessary to address changing needs.
- Implement pull printing, if appropriate, to the use and location of the MFD.

5.2.4 User Authentication

Authentication is essential to ensure that only authorized users have access to the network, to prevent unauthorized users from scanning and e-mailing documents, and to provide an audit trail of what was sent and by whom. Authentication also prevents users from exceeding their level of privilege. By using one device to print, scan, copy and fax you can implement a single form of authentication across all these functions resulting in an integrated security framework.

The following standards should be met:

- Implement security at each application level.
- Require authentication for people needing to fax, scan, copy or print faxes, from the MFD.
- Ensure that all e-mail can be traced back to an individual.
- Establish a timeout period to ensure that a user who fails to log off does not remain connected.

5.3 Activity Logging

By running regular activity logs, a complex and detailed picture is provided regarding how the MFD is being used and the associated network impact. This helps pre-empt potential security problems, provides the opportunity to spot any misuse of resources, and helps to keep the network optimized to closely match real user needs. Activity logging is especially important in any environment where protected information is stored and its distribution must be monitored. The campus technical support staff should:

- Ensure that logging is enabled on MFDs.
- Review logs on a regular basis.
- If there is a question or an anomaly, ensure that activity is available for review.
- Follow data retention policies for logs.

5.4 Existing MFDs Not Meeting the Standard

For devices that are currently in use and do not have the security features required by this Standard:

- If possible, purchase the necessary security modules and enable the features.
- If security features cannot be purchased or enabled, replace the device as soon as it is appropriate.
- Do not use and process protected data on the device until the device has the necessary security features.

5.5 MFDs Returned, Transferred or Serviced

Once data has been written to any disk drive, the potential exists for it to be retrieved – even after deletion – unless it’s been effectively overwritten or destroyed. If a MFD does not have advanced security options such as disk encryption or the ability to immediately overwrite data, the hard drive should be erased, overwritten or physically removed from machines before its transfer or disposition.

In the event of an on-site service call or off-site repair requiring the swapping of the hard drive, the hard drive being detached must be erased or overwritten before being removed from the department.

5.6 Information Security Contract Language

Third-party service providers are responsible for meeting all information security requirements of the University. To ensure this provision, all purchase requisitions, service orders, contracts or other procurement documents with vendors implementing or maintaining MFDs must contain both of the following:

a) The provisions of this document, *ITS-2013-S Standards for Utilization of Multi-function Devices*, or a clear reference to its web link: http://www.calstatela.edu/its/itsecurity/guidelines.

b) The completed form *ITS-2827 Information Security Contract Language for Third-party Service Providers with Direct Data Access* template, available at http://www.calstatela.edu/its/forms/ITS-2827_Contract_Language_forThird_Parties_with_Direct_Data_Access.doc.

5.7 Other Vendor Options

The campus has multiple vendors and models of MFDs in place. Since options for securing MFDs can vary depending on the device and the manufacturer, campus technical support staff should review the additional options provided by the vendor of their MFD to improve device security.

6 Contacts

a. For questions regarding specific department procedures, contact the department administrator.

b. Address questions regarding these standards to: ITSecurity@calstatela.edu.

7 Applicable Federal and State Laws and Regulations

Federal	Title
NA	
State	**Title**
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that provides information on safeguarding personal information.
SB 1386	**California Personal Information Privacy Act, SB 1386** http://www.info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb1386_bill_20020926_chaptered.html This bill modified Civil Code Section 1798.29 to require notification to individuals whose personal information is or is assumed to have been acquired by unauthorized individuals.

8 Related Documents and Resources

ID/Control #	Title
ITS-1006-G	**User Guidelines for Securing Offices, Workspaces, and Documents** http://www.calstatela.edu/its/itsecurity/guidelines This guideline is intended to help the campus community protect offices, machines, devices and documents from unauthorized access to confidential, personal and proprietary information.
ITS-1017-G	**User Guidelines for Safe Disposal of Electronic Storage Media** http://www.calstatela.edu/its/itsecurity/guidelines This guideline outlines the steps departments and business units, students, faculty and staff should take to remove data and software and appropriately dispose of electronic equipment/devices.
ITS-1021-G	**User Guidelines for Data Sanitization** http://www.calstatela.edu/its/itsecurity/guidelines This guideline defines the appropriate data sanitization tools and procedures to meet security standards.
ITS-1027-G	**User Guidelines for Encryption Security** http://www.calstatela.edu/its/itsecurity/guidelines This guideline provides information on approved encryption algorithms, recommended encryption products, and specific encryption tools and practices.
ITS-2006-S	**Information Classification, Handling and Disposal** http://www.calstatela.edu/its/itsecurity/guidelines This standard identifies the three levels of information classification and outlines the best practices for handling and disposing of protected data.
ITS-2008-S	**Password Standards** http://www.calstatela.edu/its/itsecurity/guidelines This standard provides guidance to all users regarding the security and management of passwords.
Administrative Procedure 707	**Record Retention, Management and Disposition** http://www.calstatela.edu/univ/admfin/procedures/707/707.pdf This procedure establishes policy for the secure management of University records and the transfer of University records to the State Records Center, the retrieval of stored records and the destruction of obsolete records.

ID/Control #	Title
California Office of Information Security	**Security Considerations for Multi-function Devices (MFD)** http://www.cio.ca.gov/OIS/Government/documents/pdf/Security_Considerations_for_Multi-Function_Devices_(MFD).pdf#search=security%20considerations%20for%20multi&view=FitH&pagemode=none -- 2010-06-02 This document specifies good business practices for Multi-function Devices (MFD).
NIST	**Guidelines for Media Sanitization – Special Publication 800-88** http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf This guide assists organizations and system owners in making practical sanitization decisions based on the level of confidentiality of their information.
NIST	**National Checklist Program** http://www.nist.gov/itl/csd/set/ncp.cfm The National Checklist Program is the U.S. government repository of publicly available security checklists that provide detailed low-level guidance on setting the security configuration of operating systems and applications.