Subject:	Server Security Standards
Standards Number:	103
Effective Date:	4/12/2019
Revised Date:	12/9/2019
Responsible Authority:	Information Security Office
Pages:	9

ACCOUNTABILITY/APPLICABILITY:

These standards apply to all University of Central Florida owned servers connected to the university network via physical, wireless, or VPN connections as well as servers hosted with a cloud vendor. These standards should provide UCF System Administrators an understanding on what security configurations should be applied to university servers in order to bring them into compliance with UCF security policies as well as state and federal regulatory requirements.

STANDARDS STATEMENT:

The purpose of this document is to establish minimum-security standards that should be applied to all university servers in order to maintain the confidentiality, integrity, and availability of university information systems. All security controls should be proportional to the data processed by the system. The following controls are recommended for all systems; however, controls denoted with an 'X' are required.

Any exception to the standards must be documented and approved by the Information Security Office in advance.

STANDARDS:

These categories and standards align with the Center for Internet Security (CIS) Critical Security Controls (CSC) and NIST cybersecurity standards.

Effective implementation of the following standards does not imply a completely secure system.

Note: An 'X' indicates a requirement to implement the given security control if the corresponding data type is present on the system.

Security Control 1: Inventory and Control of Hardware Assets (CSC 1)					
#	**Name**	**Security Control**	**Data Classification**		
			Unrestricted	**Restricted**	**Highly Restricted**

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

1.1	Asset Inventory	Maintain an accurate inventory of all physical and virtual servers. Ensure that the asset inventory records IP addresses, hardware addresses, machine names, serial numbers, system owners, department names, and a description for each asset. **Note**: Cloud environments *may* document computer objects by default.	**X**	**X**	**X**
1.2	Equipment Disposal	All university-owned equipment must go through Surplus Property for disposal.	**X**	**X**	**X**
1.3	Equipment Transfers	All university-owned equipment prior to transferring to another department without going through Surplus must be wiped to prevent data disclosure.	**X**	**X**	**X**

Security Control 2: Inventory and Control of Software Assets (CSC 2)

#	Name	Security Control	Data Classification		
			Unrestricted	**Restricted**	**Highly Restricted**
2.1	Software Inventory	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	**X**	**X**	**X**
2.2	Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the latest vendor-supported version. See the University Information Security *Patch Management Standard.*	**X**	**X**	**X**
2.3	Physically or Logically Separate High-Risk Applications	Physically or logically separate application servers, database servers, and web servers.			**X**

Security Control 3: Vulnerability Management (CSC 3)

#	Name	Security Control	Data Classification		
			Unrestricted	**Restricted**	**Highly Restricted**
3.1	Vulnerability Scanning	Deploy remote or local vulnerability scanners and perform reoccurring vulnerability scans on systems.	**X**	**X**	**X**
3.2	Dedicated Scanning Accounts	Use a dedicated account for authenticated vulnerability scans. This account should not	**X**	**X**	**X**

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

		be used for any other administrative activities.			
Security Control 4: Identity Access Management (CSC 4)					
#	**Name**	**Security Control**	**Data Classification**		
			Unrestricted	**Restricted**	**Highly Restricted**
4.1	Password Policy	All passwords must adhere to University Information Security Password Standard *501 Password Standards.*	**X**	**X**	**X**
4.2	User Authentication	End-users logging into applications must be authenticated to the NET domain. To provide administrative access systems	**X**	**X**	**X**
4.3	Access Control	Use the principal of least privilege when setting access controls for users and system services.	**X**	**X**	**X**
4.4	Secure Desktop	Switch to the secure desktop when prompting users for elevation.	**X**	**X**	**X**
4.5	Dedicated Administrative Accounts	Dedicated administrative accounts must be used for any elevated activities. This account should only be used for administrative activities and not Internet browsing, email, or similar activities. Admins must be challenged by Multi Factor Authentication when elevating privileges.	**X**	**X**	**X**
4.6	Centralized Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	**X**	**X**	**X**
4.7	Multi-Factor Authentication (MFA)	Use multi-factor authentication to protect applications that handle highly-restricted information.			**X**
4.8	Local Administrative Accounts	Local administrator accounts on servers should have unique passwords and keys. Local administrative accounts must not be used in place of a dedicated administrator account.	**X**	**X**	**X**
4.9	Key Management	All SSH keys must be stored in Secret Server	**X**	**X**	**X**
Security Control 5: Secure Configuration for Hardware and Software (CSC 5)					

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

#	Name	Security Control	Data Classification		
			Unrestricted	Restricted	Highly Restricted
5.1	Standard Secure Configurations	All systems must be deployed using a standard secure image with a standard pre-secured configuration. Standard configurations must meet the requirements prescribed in this standard or otherwise meet or exceed the Center for Internet Security (CIS) Level 1 System Standards. The standard configurations should be periodically audited/scanned to ensure ongoing compliance.	**X**	**X**	**X**
5.2	Patch Management	Regularly deploy software updates to ensure that all systems have the most recent security patches installed. See the University Information Security *Patch Management Standard.*	**X**	**X**	**X**
5.3	BIOS/UEFI Password	Set unique administrator passwords to prevent unauthorized users from accessing BIOS or UEFI settings.	**X**	**X**	**X**
5.4	Remote System Administration: Encryption	All remote system administration should be done through an encrypted channel such as RDP or SSH.	**X**	**X**	**X**
5.5	Remote System Administration: Access	RDP, SSH, and other remote administration ports should not be accessible from the internet or general internal networks. Instead, access to these protocols should be via a central authentication point like a jumpbox or VPN with MFA.	**X**	**X**	**X**
5.6	Remote System Administration: Multi-Factor Authentication (MFA)	Remote connections to servers must prompt users for MFA before allowing the remote user to connect to the server, or alternatively through a jumpbox or VPN with MFA.	**X**	**X**	**X**
5.7	Remote System Administration: Inactivity Timeout	The inactivity timeout limit for remote sessions should be set to 4 hours or less for Unix systems and 10 hours or less for Windows systems.	**X**	**X**	**X**
5.8	System Banner	All systems that support interactive login must prompt users with the University Logon Banner. See the University Information Security Standard *107 System Banner Standards.*	**X**	**X**	**X**
Security Control 6: Monitoring and Analysis of Audit Logs (CSC 6)					

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

#	Name	Security Control	Data Classification		
			Unrestricted	Restricted	Highly Restricted
6.1	Synchronized NTP Sources	To keep system log timestamps consistent, utilize the trusted UCF NTP sources to retrieve time information on a regular basis. **NTP Sources:** time.ucf.edu time2.ucf.edu	**X**	**X**	**X**
6.2	Logged Events	The following event types should be logged: • Account Authentications • Account Lockouts • User Account Management • Elevated Privilege Use • Network Connections • Security Policy Changes • Malware Events	**X**	**X**	**X**
6.3	Enable Detailed Logging	Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	**X**	**X**	**X**
6.4	Log Retention	System administrators should aim to keep logs for as long as required by state and federal regulations. If a system's disk storage is full the device should deal with the logs in one of the following ways: 1. Forward required logs to the University's central Security Information and Event Management (SIEM) tool, overwrite the oldest logs then continue logging. Contact soc@ucf.edu for more details. 2. Backup required logs to a remote file share, overwrite the oldest logs then continue logging. 3. Backup logs to a remote file share, purge local logs then continue logging.	**X**	**X**	**X**

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

6.5	Central Log Management	Ensure that appropriate logs are being forwarded to the University's central Security Information and Event Management (SIEM) tool. Contact soc@ucf.edu for more details.	**X**	**X**	**X**

Security Control 7: Web Browser Protections (CSC 7)

#	Name	Security Control	Data Classification		
			Unrestricted	**Restricted**	**Highly Restricted**
7.1	Ensure Use of Only Fully Supported Browsers	Ensure that only vendor-supported web browsers are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor. **Note**: Servers should not be used for browsing the Internet.	**X**	**X**	**X**

Security Control 8: Malware Defense (CSC 8)

#	Name	Security Control	Data Classification		
			Unrestricted	**Restricted**	**Highly Restricted**
8.1	Anti-Malware Software	Anti-malware software should be installed, enabled, and kept up to date. Malware signatures should be updated regularly	**X**	**X**	**X**
8.2	Removable Media Anti-Malware Scanning	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	**X**	**X**	**X**
8.3	Disable Auto-run	Configure devices to not auto-run content from removable media.	**X**	**X**	**X**
8.4	Anti-Malware Logging	Send all malware detection events to the University's System Center Operations Manager (SCOM) tool for analysis and alerting.	**X**	**X**	**X**

Security Control 9: Control of Network Ports, Protocols, and Services (CSC 9)

#	Name	Security Control	Data Classification		
			Unrestricted	**Restricted**	**Highly Restricted**
9.1	Network Ports, Services and Protocol Inventory	System owners must maintain an accurate and up to date inventory if any network ports, services, and protocols are required.	**X**	**X**	**X**

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

9.2	Enable Host-level Firewalls	Enable host firewalls, or if available, enable virtual host network firewalls, and configure it to default-deny mode that drops all traffic except established sessions and the services and ports that are explicitly allowed.	**X**	**X**	**X**
9.3	Ensure Only Approved Ports, Protocols and Services Are Running	Ensure that only approved network ports, protocols, and services are running on each system.	**X**	**X**	**X**
9.4	Disable Unsupported Protocols	Disable or remove any unsupported, outdated, or insecure protocols such as but not limited to SMBv1, SNMP, SSLv2, SSLv3, and NTLMv1.	**X**	**X**	**X**
Security Control 10: Data Recovery (CSC 10)					
#	**Name**	**Security Control**	**Data Classification**		
			Unrestricted	**Restricted**	**Highly Restricted**
10.1	Regular Back Ups	Ensure that critical system data is automatically backed up to a University approved backup location.	**X**	**X**	**X**

DEFINITIONS:

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

BIOS: The Basic Input Output System contains instructions to load the computer's operating system into memory and finish the boot-up process.

Host-Based Firewall: A firewall that *locally* monitors and controls incoming and outgoing network traffic on a system.

Jumpbox/Jumpserver/Jumphost: A system on a network that is used to access and manage devices in a separate security zone.

Malware: A type of malicious software or unwanted program designed to infect computer systems, sometimes causing damage to the infected systems, or stealing information (e.g., computer virus, spyware, etc.)

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

NT LAN Manager (NTLM): A Microsoft Windows protocol that provides authentication to users.

Principal of Least Privilege: A concept that states to provide access to only the information and resources that are necessary for its legitimate purpose.

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

Security information and event management (SIEM): A security tool that provides real-time monitoring, correlation of events, and notifications.

Server Message Block (SMB): A Windows service that is used for sharing access to files, printer, serial ports, and other communications between networked systems.

Simple Network Management Protocol (SNMP): A protocol used for collecting, organizing, and modifying information about managed networked devices.

UEFI: Unified Extensible Firmware Interface replaces the BIOS in newer computers and provides additional functionality.

Vulnerability: A weakness that can be accidentally triggered or intentionally exploited.

RELATED DOCUMENTS:

1. 4-007.1 *Security of Mobile Computing, Data Storage, and Communication Devices* policy
    a. https://policies.ucf.edu/
2. 4-008.1 *Data Classification and Protection* policy
    a. https://policies.ucf.edu/
3. 105 *Patch Management Standards*
    a. https://infosec.ucf.edu/policiesandstandards/
4. 107 *System Banner Standards*
    a. https://infosec.ucf.edu/policiesandstandards/
5. 501 *Passwords Standards*
    a. https://infosec.ucf.edu/policiesandstandards/
6. CIS System Benchmarks
    a. http://benchmarks.cisecurity.org/
7. NIST Cybersecurity Standards
    a. https://csrc.nist.gov/publications/sp800

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
5/31/2019	• **Item 6.2 -** Revised the list of logged events.
12/9/2019	• **Accountability Statement -** Added verbiage about cloud vendors • **Definitions -** Added definitions for jumpbox and host-based firewall • **Item 1.3 –** Added new section "Equipment Transfers" • **Items 5.4 – 5.6 -** Added prefix "Remote System Administration:" to items 5.4 – 5.6 • **Item 4.5 -** Added MFA requirement verbiage for Dedicated Administrative Accounts • **Item 5.5 -** Added clause "remote administration ports should not be accessible from the internet"

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL
(For use by the Information Security Office)

Standards Number: *103*

Initiating Office: Information Security Office

Chief Information Security Officer: *Chris Vakhordjian*

Signature: chrisv chrisv dc=edu, dc=ucf, dc=net, ou=People, cn=chrisv, email=Chris.Vakhordjian@ucf.edu 2020.03.10 16:15:07 -04'00' Date: _____

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