UNIVERSITY
OF
CALIFORNIA

UCOP
ITS
Systemwide CISO Office
Systemwide IT Policy

UC Minimum Security Standard

Revision History

Date:	By:	Contact Information:	Description:
08/8/2017	Robert Smith	robert.smith@ucop.edu	Approved by the CISOs for consideration by ITLC and shared governance. Interim until approved by ITLC.

TABLE OF CONTENTS

UC Minimum Security Standard - Overview

Description and Purpose:

This UC Standard defines minimum security requirements for devices connected to Location networks.

This Standard must be used in conjunction with UC's information security policy, BFB-IS-3 Electronic Information Security.

Scope:

This Standard applies to all of the following:

- All UC campuses and medical centers, the UC Office of the President, UC Agriculture and Natural Resources, UC-managed national laboratories and all other UC locations (Locations).
- All Workforce Members, Suppliers, Service Providers and other authorized users of Institutional Information and IT Resources.
- All use of Institutional Information, independent of the location (physical or cloud) or ownership of any device or account that is used to store, access, process, transmit or control Institutional Information.
- All devices, independent of their location or ownership, when connected to a UC network or cloud service by Workforce Members, Service Providers and authorized users, which may include Suppliers providing Workforce Members, used to store or process Institutional Information.
- Research projects performed at any Location, and UC-sponsored work performed by any Location.

This Standard does not apply to the following:

- End-user devices used and owned by the public.
- End-user devices used and owned by students for purposes of attending the University and completing projects.
- Students who are not Workforce Members.

Definitions:

Institutional Information is a term that broadly describes all data and information created, received and collected by UC. Workforce Member is a term that broadly describes any of the following: employee, faculty, staff, volunteer, contractor, researcher, student worker, student supporting/performing research, medical center staff/personnel, clinician, student intern, student volunteer or person working for UC in any capacity or through other augmentation to UC staffing levels.

All other capitalized terms in this Standard are defined in the UC IT Policy Glossary.

Organization:

This Standard is organized into two sections for two different audiences:

- Section I lists key security controls that apply to all Workforce Members when other IS-3 or Location policies are not applicable. The requirements can also be found at https://security.ucop.edu/policies/index.html. The ISO 27002 column is for compliance tracking and does not apply to end-users. The column is not displayed on the website.

- Section II lists additional security controls that apply to IT professionals or those whose core job responsibilities include IT functions.

The controls outlined in this Standard are systemwide minimum requirements. Locations may require additional controls or use alternative approaches, check with your local IT support group, CISO or Compliance Officer. Links to those resources are found on the left side of this page: https://security.ucop.edu/services/index.html.

Requirements:

The requirements for this Standard are listed in the tables on the following pages.

When Institutional Information classified at Protection Level 3 or higher is stored, processed or transmitted, additional controls must be applied. See IS-3, Part III, Sections 6 to 18. Units must ensure the correct controls are applied.

When Institutional Information or IT Resources are classified at Availability Level 3 or higher, additional controls must be applied.

Section I

Minimum Security Standard for Workforce Members and the devices they control

Required - ✓, Recommended - ◆, Not Required - ◪

All Workforce Members are responsible for ensuring the protection of Institutional Information and IT Resources.

The following table outlines 12 security requirements that help manage cybersecurity risk. Workforce Members can help keep UC secure by meeting these requirements. There requirements help reduce cyber security risk and reduce the likelihood of costly incidents.

#	Topic	Requirement	Tips	Mobile	Windows	Mac OS	Linux	ISO 27002:2013 Reference
1	Anti-malware	Anti-malware software must be installed and running up-to-date definitions.	Enable real-time protection and regular full scans.	◆	✓	✓	◆	12.2
2	Patching	Supported security patches must be applied to all operating systems and applications.	Where possible, use automatic updating or connect to your IT department patching and upgrade service. Apply patching as soon as possible as it quickly reduces risk.	✓	✓	✓	✓	12.6
3	Local admin or Administrator	Non-privileged user accounts must be used and only elevated to root	Perform routine and daily activities using non-privileged accounts.	◪	✓	✓	✓	9.2.3

#	Topic	Requirement	Tips	Mobile	Windows	Mac OS	Linux	ISO 27002:2013 Reference
		or Administrator when necessary.	Use Administrator on Windows/Mac OS or Root/SU on Linux or UNIX only for a specific administrative action. Log out of the account after completing the action. Contact your Location help desk or IT support center to set up root or Administrator accounts if necessary.					
4	Encryption	Laptops and mobile devices must be encrypted. Separately, Institutional Information classified at Protection Level 3 or higher must be encrypted when stored on Laptops and mobile devices.	Use the approved encryption method for your Location. If you don't need it, don't store it. If you need to store it, encrypt it. Device-level encryption is the best option. If the device is not encrypted, encrypt any Institutional Information classified at Protection Level 3 or higher when stored on Laptops and mobile devices.	✓	✓	✓	✓	8.3.1, 10.1, 9.4.2, 10.1, 13.2

#	Topic	Requirement	Tips	Mobile	Windows	Mac OS	Linux	ISO 27002:2013 Reference
5	Session timeout	Devices used to store or access Institutional Information or IT Resources classified at Protection Level 2 or higher must employ lockout/screen-lock mechanisms or session timeout or to block access after a defined period of inactivity (15 minutes or Location limit). Mechanisms must require re-authentication before a return to interactive use.	Enable the locking screensaver on Windows or Mac OS. Enable inactivity timeout on mobile devices. Use TMOUT or another method to automatically log out on LINUX or UNIX.	✓	✓	✓	✓	9.3, 11.2
6	Password/PIN lock	Secure devices with a strong password, PIN, smart card or biometric lock.	Strong passwords and PINs are one of UC's best defenses against unauthorized access. Consult Location resources for guidance on creating strong passwords/PINs, smart card or biometric lock that complies with the UC Account and Authentication Management Standard. Strong passwords are 10-64 characters in length	✓	✓	✓	✓	, 9.2.4, 9.2.6, 9.3, 9.3.1, 9.4.2, 9.4.3,11.2

#	Topic	Requirement	Tips	Mobile	Windows	Mac OS	Linux	ISO 27002:2013 Reference
			and include upper and lowercase letters, numbers and special characters. Do not share passwords or PINs, and do not use common or similar passwords across accounts. Do not use your UC username and password for personal accounts. Do not use default passwords, and change default passwords immediately. Never use your username, “password,” “123456,” “12345678,” “qwerty,” common words, phrases or your name as your password.					
7	Physical security	Devices and Institutional Information must be physically secured.	Use physical security cables to protect against theft or loss of valuable information from your workplace or vehicle. Lock devices in a cabinet	✓	✓	✓	✓	7.0, 9.3, 11.2, 11.2.9

#	Topic	Requirement	Tips	Mobile	Windows	Mac OS	Linux	ISO 27002:2013 Reference
			at the end of the day/shift. Do not leave unencrypted devices unattended.					
8	Backup and recovery	Institutional Information classified at Availability Level 3 or higher must be backed up and recoverable. Backups must be protected according to the classification level of the information they contain.	Ensure the backup plan is consistent with business, regulatory and records management requirements.	✓	✓	✓	✓	12.3
9	Encrypt portable media	Backups and portable media containing Institutional Information classified at Protection Level 4 must be encrypted and safely stored.	Encrypt all portable media and backups whenever possible. Lost or stolen media is a common cause of reportable data breaches. It's a good practice to encrypt Institutional Information classified at Protection Level 3 too. Some Locations require encryption for Institutional Information classified at Protection Level when stored on portable media!	✓	✓	✓	✓	8.3.1, 12.3

#	Topic	Requirement	Tips	Mobile	Windows	Mac OS	Linux	ISO 27002:2013 Reference
10	Host-based firewall	If host-based firewall software is available on a device, it must be running and configured to block all inbound traffic that is not explicitly required for the intended use of the device.	Use the firewalls that come with Windows, many popular anti-malware applications, Apple and Linux. Default settings are typically acceptable.	◪	✓	✓	✓	6.2.2, 12.2
11	Approval and inventory	Make sure devices can be secured before making a purchasing decision. Make sure IT Resources and Institutional Information are appropriately recorded in Location inventory.	Consult your Location IT department or online resources to determine whether a device requires approval and recording in inventory. Many security breaches can be prevented or their impact minimized if your IT department is aware of your device and what's stored on it.	✓	✓	✓	✓	8.1.1, 8.1.2, 12.6.1, 18.1.3,
12	Supported Operating Systems	Run a version of the operating system that is supported by the vendor.	Do not use end-of-life operating systems such as Windows XP, Server 2003 or Vista. They no longer receive security patches and are vulnerable to compromise.	✓	✓	✓	✓	12.5, 12.6.

End of Section I.

Section II

Minimum Security Standard for Other Network-Connected Devices

These include, but are not limited to, servers, appliances, applications, Internet of Things (IoT) and other devices used to process, store and transmit UC Institutional Information.

This section applies to IT professionals and Workforce Members who administer and install systems.

Required - ✓, Recommended - ◆, Not required - ◪

IT Workforce Members play an important role in ensuring the protection of Institutional Information and IT Resources.

The table below outlines five key security controls that help manage cyber security risk. IT Workforce Members can help keep UC secure by following these controls and understanding the risks, threats, cost and incidents associated with securing Institutional Information.

Additional controls apply if the Institutional Information created, processed or stored is classified at Protection Level 2 or higher and/or Availability Level 2 or higher. IS-3, the Location CISO or a Location Risk Treatment Plan can provide the applicable security control set and approach.

#	Topic	Requirement	Tips	Servers	Applications	Other	ISO 27002:2013
1	**Minimum Security Standard for Workforce Members and**	Comply with the minimum security standards in Section I.		✓	✓	✓	NA

#	Topic	Requirement	Tips	Servers	Applications	Other	ISO 27002:2013
	the devices they control						
2	Network services	Network services must be secured as follows: • Only network services needed to support work must be enabled. All other services must be disabled or removed. • Network access must be limited to devices that need access for the approved use case. • Anonymous logins or use of HTTP to log in must not be allowed. • An encrypted connection (i.e. HTTPS, SSH or cryptographically strong protocol) must be used for all authentication sessions and subsequent access.	Do not use network services that are unnecessary and/or exposed to the Internet, as they increase the risk of compromise. Use secure versions of applications and services.	✓	✓	✓	9.1.1, 9.1.2, 9.2.1, 9.4.1,13.1.1,
3	Network bridging	Devices or servers must not be configured to bridge one security classification to another	Two network interfaces are common in both	✓	✓	✓	12.4.1, 13.1.2, 13.1.3, 13.2.1, 18.1.3, 18.2.3

#	Topic	Requirement	Tips	Servers	Applications	Other	ISO 27002:2013
		in an unauthorized manner (also known as split tunneling) or bridge networks that are intended to be segmented (also known as network bridging).	physical and virtual machine networking. This is typically called “Dual Home.” Make sure both network interfaces are appropriately protected and segmented and use is approved by the CISO. If you’re managing remotely, Location-approved “jump boxes” or “bastion hosts” are permitted.				
4	Changing default credentials	All default passwords included as part of the initial setup of any system must be changed as soon as practical, and in all cases prior to the system being	Various systems support different capabilities for password complexity.	✓	✓	✓	9.2.4

#	Topic	Requirement	Tips	Servers	Applications	Other	ISO 27002:2013
		moved to production. If no password is set, one must be set that meets the UC Account and Authentication Management Standard.	See the Authentication Management Standard for guidance on creating strong passwords.				
5	Limit access to authorized users	Access to Institutional Information and IT Resources must be limited to Unit authorized users. Prevent unauthorized use of IT Resources.	Only network proxy or gateway services whose configuration and use have been approved by the Location are allowed on the Location network. Do not use/allow: • Open mail relays. • Unauthorized proxy servers. • Open or writable file shares not intended for	✓	✓	✓	8.1.1, 8.1.2, 9.2, 12.5.1, 12.6.1

#	Topic	Requirement	Tips	Servers	Applications	Other	ISO 27002:2013
			public use. • Writable web applications not intended for public use.				

End of Section II.

References

Standards

ISO 27002:2013 - references supplied above.

UC IT Policy Glossary

Use the UC IT Policy Glossary for defined terms.

UC Policy

BFB-IS-3 Electronic Information Security