UNIVERSITY OF OREGON

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

UO Minimum Information Security Technical Controls Standard

Purpose

This standard outlines the minimum controls for protecting information assets, as required by the Information Asset Classification and Management Policy (IV.06.02). The purpose of requirements identified herein is to reduce risks to the confidentiality, integrity and availability of University data and systems ("information assets") and to protect the privacy of members of the University community.

Scope

This standard applies to all users with access to University information assets, and all devices that store, process or transmit University data.

Standard

All users with access to University information assets, and all devices that store, process or transmit University data shall meet the following minimum controls for protecting University information assets, unless an exception is approved by the Information Security Office (ISO).

Exception Request

There may be valid reasons why a given required control cannot be met; e.g., technology limitations, conflict with other controls, the presence of compensating controls, lack of funding, and financial needs that exceed the potential risk of not implementing the control. Exception requests must be submitted to ISO detailing reasons the control cannot be met and proposing compensating controls to minimize the risk caused by not meeting the controls. Exceptions request should be submitted to infosec@uoregon.edu.

UNIVERSITY OF OREGON

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

Compliance Management

The ISO shall implement processes and services to continuously monitor information systems for compliance with this standard.

Policy Violation

Non-compliance with this standard is a violation of the University Information Asset Classification Policy (IV.06.02) and are subject to University sanctions. In cases where noncompliance poses serious risks to University information assets, ISO may take steps to mitigate such risks including temporarily quarantining vulnerable or compromised computers, temporarily disabling affected network ports, blocking known bad or compromised IP addresses, disabling affected network ports, blocking known bad or compromised IP addresses, disabling compromised user accounts, or other actions as necessary to protect University information assets and users.

Definitions

Mandatory Controls must be applied as described in this standard.

Recommendation Controls should be applied as described in this standard.

Compensating Controls are alternative controls put in place to meet or exceed the security requirement, typically to address difficulty or impracticality in implementing the required control. Typically, compensating controls are temporary until it becomes practical to implement the required controls.

UNIVERSITY OF OREGON

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

Section I - UO Minimum Technical Security Controls by Classification

The following technical security controls must be implemented for University-owned systems or vendor/partner systems that store, process or transmit University data in accordance with the classification of the system. Personally-owned systems (e.g., BYOD, home computers, personal phones, etc.) that are used to store, process or transmit University data are required to meet or exceed these standards, before such use is approved by ISO.

Servers

	Information System Classification **M** – Mandatory; **R** – Recommended; **NR** – Not Required			
Control	**High Risk (Red)**	**Moderate Risk (Amber)**	**Low Risk (Green)**	**Applicable Service**
IDENTIFICATION Controls				
UO.ID.1 Configuration Management System (CMS): Registration	M	M	M	SCCM, JAMF, Puppet, NetDot
UO.ID.2 Configuration Management System (CMS): Management (OS)	M	M	M	SCCM, JAMF, Puppet, CMDB
UO.ID.3 Configuration Management System (CMS): Management (Apps)	M	M	R	SCCM, JAMF, Puppet, CMDB, Ansible
UO.ID.4 Vulnerability Scanning	M	M	M	ISO Vulnerability Scanning Service
UO.ID.5 Penetration Testing	M	R	NR	
PROTECTION Controls				
UO.PR.1 Physical Security	M	R	NR	Datacenter, approved Cloud
UO.PR.8 Auto-lock Screens	M	M	R	
UO.PR.3 System Hardening	M	M	R	
UO.PR.4 Security Baseline Configuration	M	M	R	ISO CIS Baseline
UO.PR.5 Security Updates	M	M	M	SCCM, JAMF, Puppet
UO.PR.6 Application Blocklist	M	R	NR	
UO.PR.7 Anti-malware (include Antivirus)	M	M	M	McAfee
UO.PR.8 Auto-lock system consoles	M	M	M	
UO.PR.9 Firewall (Host-based)	R	R	R	
UO.PR.10 Firewall (Network)	M	M	R	
UO.PR.11 Encryption: Data-at-Rest	M	R	NR	
UO.PR.12 Encryption: Data-in-Transit	M	M	R	
UO.PR.14 User Access Control: Unique Account	M	M	R	Duck IDs

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

UO.PR.15 User Access Control: Least Privilege Access	M	M	M	
UO.PR.16 User Access Control: Access Approval	M	M	M	
UO.PR.17 User Access Control: Authentication	M	M	M	Active Director, LDAP, SAML
UO.PR.18 User Access Control: Limit Failed Login Attempts	M	M	M	
UO.PR.19 User Access Control: Inactive Session Timeout	M	R	R	
UO.PR.20 User Access Control: Two-Factor Authentication	M	M	R	DUO 2FA
UO.PR.21 User Access Control: Remote Privileged Access Session Security	M	M	R	SSH, SCP, sFTP, VPN, TLS, IPSec VPN
DETECTION Controls				
UO.DE.1 Logging and Retention	M	R	NR	ISO Logging & Security Analytics
UO.DE.2 Log Monitoring	M	R	NR	SIEM
UO.DE.3 File Integrity Monitoring	M	R	NR	
RECOVERY Controls				
UO.RC.1 Incident Recovery: Backup & Recovery	M	R	R	
UO.RC.2 Incident Recovery: Restoration Testing	M	R	R	

Non-mobile Workstations

	Information System Classification **M** – Mandatory; **R** – Recommended; **NR** – Not Required			
Control	**High Risk (Red)**	**Moderate Risk (Amber)**	**Low Risk (Green)**	**Applicable Service**
IDENTIFICATION Controls				
UO.ID.1 Configuration Management System (CMS): Registration	M	M	M	SCCM, JAMF, Puppet, NetDot
UO.ID.2 Configuration Management System (CMS): Management (OS)	M	M	M	SCCM, JAMF, Puppet, CMDB
UO.ID.3 Configuration Management System (CMS): Management (Apps)	M	M	R	SCCM, JAMF, Puppet, CMDB, Ansible
UO.ID.4 Vulnerability Scanning	M	M	M	ISO Vulnerability Scanning Service
UO.ID.5 Penetration Testing	R	NR	NR	
PROTECTION Controls				
UO.PR.1 Physical Security	M	R	NR	Virtual desktops
UO.PR.8 Auto-lock Screens	M	M	R	
UO.PR.4 Security Baseline Configuration	M	R	R	UO CIS Baseline

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

UO.PR.5 Security Updates	M	M	R	SCCM, JAMF, Puppet
UO.PR.6 Application Blocklist	M	M	R	OS ACL, Consider different lists per risk
UO.PR.7 Anti-malware (including antivirus)	M	M	M	McAfee
UO.PR.9 Firewall (Host-based)	R	R	R	
UO.PR.10 Firewall (Network)	M	M	R	
UO.PR.15 User Access Control: Least Privilege Access	M	M	R	
UO.PR.17 User Access Control: Authentication	M	M	R	Active Directory, LDAP, Shibboleth/SAML
UO.PR.18 User Access Control: Limit Failed Login Attempts	M	M	R	
UO.PR.20 User Access Control: Two-Factor Authentication	M	M	R	e.g., DUO 2FA
UO.PR.21 User Access Control: Remote Privileged Access Session Security	M	M	R	IPSec VPN, SSH, TLS
UO.PR.11 Encryption: Data-at-Rest	M	R	NR	
UO.PR.12 Encryption: Data-in-Transit	M	R	NR	
UO.PR.13 Encryption: Full Disk Encryption	M	M	R	
UO.PR.22 Web Reputation Filtering	M	R	R	
DETECTION Controls				
UO.DE.1 Logging and Retention	M	R	NR	ISO Logging & Security Analytics Service
UO.DE.2 Log Monitoring	M	R	NR	SIEM
RECOVERY Controls				
UO.RC.1 Incident Recovery: Backup & Recovery	M	R	R	

UNIVERSITY OF OREGON

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

Application Systems: Web-layer, middleware, databases, etc. -

	Information System Classification **M** – Mandatory; **R** – Recommended; **NR** – Not Required			
Control	**High Risk (Red)**	**Moderate Risk (Amber)**	**Low Risk (Green)**	**Applicable Service**
IDENTIFICATION Controls				
UO.ID.3 Configuration Management System (CMS): Management (Apps)	M	M	NR	
UO.ID.4 Vulnerability Scanning (Web)	M	R	R	ISO Vulnerability Scanning Service
UO.ID.5 Penetration Testing	M	R	NR	
PROTECTION Controls				
UO.PR.3 System Hardening (app layer)	M	M	M	
UO.PR.5 Security Updates	M	M	M	
UO.PR.12 Encryption: Data-in-Transit	M	M	NR	
UO.PR.14 User Access Control: Unique Account	M	R	NR	Duck ID
UO.PR.15 User Access Control: Least Privilege Access	M	R	R	
UO.PR.16 User Access Control: Access Approval	M	M	R	
UO.PR.17 User Access Control: Authentication	M	M	R	Active Directory, LDAP, SAML, another Managed Authentication System
UO.PR.18 User Access Control: Limit Failed Login Attempts	M	R	R	
UO.PR.19 User Access Control: Inactive Session Timeout	M	R	NR	
UO.PR.20 User Access Control: Two-Factor Authentication	M	R	NR	DUO 2FA
UO.PR.21 User Access Control: Remote Privileged Access Session Security	M	M	R	VPN, TLS, etc.
DETECTION Controls				
UO.DE.1 Logging and Retention	M	R	R	ISO Logging & Security Analytics
UO.DE.2 Log Monitoring	M	R	R	SIEM for high- and medium-risk systems

UNIVERSITY OF OREGON

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

Network Infrastructure Devices: Routers, Firewalls, Switches, APs, etc.

	Information System Classification **M** – Mandatory; **R** – Recommended; **NR** – Not Required			
Control	**High Risk (Red)**	**Moderate Risk (Amber)**	**Low Risk (Green)**	**Applicable Service**
IDENTIFICATION Controls				
UO.ID.2 Configuration Management System (CMS): Management (OS)	M	M	M	
UO.ID.4 Vulnerability Scanning	M	M	M	ISO Vulnerability Scanning Service
UO.ID.5 Penetration Testing	M	M	M	
PROTECTION Controls				
UO.PR.1 Physical Security	M	M	M	Datacenter, Network core node PoP
UO.PR.2 Wall Jack Access Control	M	M	M	
UO.PR.3 System Hardening	M	M	M	
UO.PR.4 Security Baseline	M	M	M	UO CIS Baseline
UO.PR.5 Security Updates	M	M	M	
UO.PR.11 Encryption: Data-at-Rest	M	R	NR	
UO.PR.12 Encryption: Data-in-Transit	M	M	NR	Some exemptions for syslog
UO.PR.14 User Access Control: Unique Account	M	M	M	Duck ID
UO.PR.15 User Access Control: Least Privilege Access	M	M	M	
UO.PR.16 User Access Control: Access Approval	M	M	M	
UO.PR.17 User Access Control: Authentication	M	M	M	Active Directory, LDAP, SAML
UO.PR.18 User Access Control: Limit Failed Login Attempts	M	R	R	
UO.PR.19 User Access Control: Inactive Session Timeout	M	M	M	
UO.PR.20 User Access Control: Two-Factor Authentication	M	M	M	DUO 2FA
UO.PR.21 User Access Control: Remote Privileged Access Session Security	M	M	M	IPSec VPN, SSH, sFTP, SCP
DETECTION Controls				
UO.DE.1 Logging and Retention	M	R	R	ISO Logging & Security Analytics
UO.DE.2 Log Monitoring	M	R	R	SIEM
RECOVERY Controls				

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

UO.RC.1 Incident Recovery: Backup & Recovery	M	M	M	
UO.RC.2 Incident Recovery: Restoration Testing	M	M	M	

UNIVERSITY OF OREGON

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

Mobile Devices: laptops, tablets, smartphones, etc.

	Information System Classification **M** – Mandatory; **R** – Recommended; **NR** – Not Required			
Control	**High Risk (Red)**	**Moderate Risk (Amber)**	**Low Risk (Green)**	**Applicable Service**
IDENTIFICATION Controls				
UO.ID.1 Configuration Management System (CMS): Registration	M	R	R	SCCM, JAMF, Puppet
UO.ID.2 Configuration Management System (CMS): Management (OS)	M	R	R	SCCM, JAMF, Puppet
UO.ID.3 Configuration Management System (CMS): Management (Apps)	M	R	NR	
UO.ID.5 Penetration Testing	R	NR	NR	
PROTECTION Controls				
UO.PR.1 Physical Security	M	R	NR	
UO.PR.8 Auto-lock Screens	M	M	M	UO Baselines
UO.PR.4 Security Baseline	M	M	M	UO Baselines
UO.PR.5 Security Updates (Automatic)	M	M	M	UO Baselines
UO.PR.6 Application Blocklist	M	R	NR	UO Baselines
UO.PR.7 Anti-malware (including antivirus)	M	M	M	McAfee
UO.PR.9 Firewall (Host-based)	M	M	R	UO Baselines
UO.PR.15 User Access Control: Lease Privilege Access	M	M	R	
UO.PR.17 User Access Control: Authentication	M	M	R	Active Director, LDAP, Shibboleth/SAML
UO.PR.18 User Access Control: Limit Failed Login Attempts	M	M	R	
UO.PR.11 Encryption: Data-at-Rest	M	M	M	
UO.PR.12 Encryption: Data-in-Transit	M	M	M	
UO.PR.13 Encryption: Full Disk Encryption	M	R	R	
RECOVERY Controls				
UO.RC.1 Incident Recovery: Backup & Recovery	M	R	NR	

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

Section II - UO Minimum Administrative Security Controls by Classification

[In Development]

UNIVERSITY OF OREGON

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

Glossary

Control Index	Control	Control Description	Security Benchmark Reference
IDENTIFICATION Controls			
UO.ID.1	**CMS: Registration**	***System shall be registered via an ISO approved Configuration Management System (CMS).*** CMS: Registration includes inventorying of system including identifiers (e.g., MAC address), IT support contact, hardware, operating system, and some software or services. CMS: Registration systems include SCCM, JAMF, or Puppet.	
UO.ID.2	**CMS: Management (OS)**	***System Operating Systems shall be managed via an ISO approved Configuration Management System (CMS).*** CMS: Management (OS) includes inventorying of system hardware, operating system, and some software or services. CMS administrators (OS) will be able to push patches and updates to systems under management. CMS administrators (OS) will also be able to push security settings and monitor for compliance for systems under management. CMS: Management (OS) systems include SCCM, JAMF, or Puppet. CMS: Management (OS) also includes CMS: Registration services.	
UO.ID.3	**CMS: Management (Apps)**	***Applications shall be managed via an ISO approved Configuration Management System (CMS).*** CMS: Management (Apps) includes inventorying of applications (or application module or components) running on a system, where practical. CMS (Apps) administrators may be able to push patches and updates to applications under management. CMS administrators (Apps) may also be able to push security settings and monitor for compliance for applications under management. CMS: Management (Apps) also includes CMS: Registration services.	
UO.ID.4	**Vulnerability Scanning**	***System shall be registered and configured for ISO ongoing vulnerability scans and identified vulnerabilities should be addressed in a timely manner not to exceed:*** • ***30 days – critical risk vulnerabilities (CVSS 9.0 - 10.0)*** • ***90 days – high risk vulnerabilities (CVSS 7.0 - 8.9)*** • ***120 days – medium risk vulnerabilities (CVSS 4.0 - 6.9)*** • ***As time allows – low risk vulnerabilities (CVSS 0.1 - 3.9)***	

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

		Our adversaries are constantly scanning our environment in search of vulnerable systems that can be exploited. Addressing ISO identified vulnerabilities in an expeditious manner significantly reduces the risk of the systems and data compromise.	
UO.ID.5	**Penetration Testing**	***The system shall be subjected to ISO conducted (or directed) penetration testing to confirm the strength of implemented controls or identify weaknesses.*** ISO will perform or coordinate penetration testing activities to confirm the effectiveness or weakness of controls to protect the system. Penetration testing exercises should only be performed following approval by the system owner.	
PROTECTION Controls			
UO.PR.1	**Physical Security**	***System shall be physically protected and monitored to prevent theft or unauthorized access to data via the system consoles or keypads.*** System should be hosted within a protected and monitored area with a secure perimeter (e.g., walls, lockable doors and windows) that protects the system from unauthorized physical access. UO datacenters should be used for hosting server devices. Endpoint devices should be kept safe to prevent them becoming loss or stolen.	
UO.PR.2	**Wall Jack Access Control**	***Require approval for connecting unmanaged and/or non-university-owned devices to UO network wall jacks.*** Unmanaged and/or non-university owned devices should be blocked from connecting to UP VLANs, unless specifically vetted and authorized by ISO. Unmanaged or non-university-owned devices can cause network loops that could disrupt availability of critical systems or loss of connectivity to entire buildings. Additionally, these devices could be used to hijack or "sniff" sensitive traffic propagating over High-Risk segments of the network.	
UO.PR.3	**System Hardening**	***Systems shall be hardened by removing unnecessary applications, services or features prior to implementation in production or assignment to users.*** Hardening a system involve removal or disabling of all unnecessary default accounts, applications (e.g., database, web server) or services (e.g., ftp service) to minimize potential vulnerabilities and the attack	

		surface of that system. In the case of applications, unused modules are features may be disabled or uninstalled as part of the hardening exercise.	
UO.PR.4	**Security Baseline**	***System shall be configured to comply with applicable ISO approved security baseline.*** ISO security baselines are developed based on industry best practices for the system in question. UO has adopted the Center for Internet Security (CIS) benchmarks to guide development of our baselines.	
UO.PR.5	**Security Updates**	***Security updates shall be applied prior to system deployment into production or assignment to users and be kept up to date thereafter.*** System should be configured to automatically download and install security updates for operating systems and third-party applications whenever possible. This will reduce vulnerabilities on the system that could be exploited to cause major security incidents.	
UO.PR.6	**Application Blocklisting**	***Application Blocklist shall be used to prevent "known bad" applications from executing.*** Application blocklists are often included as part of major operating systems to be able to limit applications executed on the system. Note: Allowlists are often more secure but may cause more inconvenience and are generally more expensive to implement.	
UO.PR.7	**Anti-malware (including antivirus)**	***Anti-malware (including antivirus) software shall be in used kept up to date.*** Anti-malware software runs continually to detect and remediate known malware (including viruses) based on heuristic or known malware signatures. To be effective, the software should always be running and should be set to automatically update signatures and rules from the manufacturer.	
UO.PR.8	**Auto-lock screens or consoles**	***Systems shall be configured to automatically lock and require a logon, pin, biometrics, or other means of authentication after being unattended or inactive for at most 5 minutes.*** Auto-lock prevents unauthorized access by passersby or others without approval for access. Inactivity timeouts may vary between ***5 and 30 minutes*** for Moderate or Low Risk systems.	
UO.PR.9	**Firewall (Host-based)**	***Host-based firewall shall be used and kept up-to-date and be configured to block inbound traffic by default.***	

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

		A host-based firewall (a.k.a, personal firewall) prevents other systems (including those on the same subnetwork or VLAN) from communicating with the system unless specifically allowed. This helps to prevent malicious software and activities to spread from nearby systems.	
UO.PR.10	**Firewall (Network)**	***Network access to or from the system shall be restricted to the least access necessary to perform required university function.*** A "stateful inspection" firewall is required and should be configured to control traffic in both directions – inbound to and out-bound from a subnetwork. This is especially required for devices that are joined to the university active directory domain. Firewall rules (especially inbound) should be configured to deny all traffic by default and create openings based on required university functions. Note: outbound filtering should address, at a minimum, well-known malicious traffic patterns (e.g., spoofed traffic, attacks on external networks).	
UO.PR.11	**Encryption: Data-at-Rest**	***Data-at-rest (stored) shall be encrypted to ensure confidentiality***. Sensitive files, records, tables or entire databases should be encrypted with the decryptions keys properly managed and changed periodically. In some cases, encryption may not be needed if ISO deemed that appropriate compensating controls have been implemented, or the risk of breach of confidentiality or integrity is substantially low. Note 1: certain combinations of Medium Risk data elements may constitute on aggregate High Risk data. Note 2: for cloud-based services, the goal is to employ the "trust no one or TNO" principle which requires decryption keys to be accessible only by approved UO personnel, thereby preventing cloud-service vendor personnel or subcontractors from accessing UO data.	
UO.PR.12	**Encryption: Data-in-Transit**	***Encrypted protocols or secure channels shall be used to transmit data to and from the system to ensure confidentiality of data and protection of UO data subjects.*** Encrypted communication prevents eavesdropping or man-in-the-middle attacks that can be used to breach the confidentiality of data. Acceptable secure communication protocols include SSH, SCP, sFTP, IPSec, TLS, VPN. *Note: in the case of connections for management or administration, data in this case may also refer to configuration files or other systems settings.*	
UO.PR.13	**Encryption: Full Disk**	***Full disk encryption shall be enabled to prevent unauthorized access to data on hard drives.***	

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

		Full disk encryption prevents access to data on hard drives without a valid decryption key (or password). E.g., if a laptop is loss or stolen, the data cannot be accessed without the decryption key. Central encryption key escrow is required to be able to assist users who forgot their encryption keys.	
UO.PR.14	**User Access Control: Unique Access Account**	***Uniquely identifiable (user ID/login name) shall be used for accessing the system to ensure accountability for user activities.*** System should be configured to use unique identifier assigned by the University (e.g., DuckID) for accessing the system. Shared IDs should be avoided to ensure that activities done on a system are individually identifiable. For cases where shared IDs must be used, additional process should be put in place to assist with unique identifiability for activities carried out on the system (e.g., ID checkout or assignment tracking process).	
UO.PR.15	**User Access Control: Least Privilege Access**	***Least privilege shall be employed to provide the minimum privileges to users and processes.*** Privileges shall be restricted and controlled in accordance with the principle of *least privilege* to reduce opportunities for unauthorized access or misuse of the system	
UO.PR.16	**User Access Control: Access Approval**	***Access and privileges shall be authorized by the system owner and reviewed at regular intervals.*** System owners should approve access to system based on the users "need to have" to perform a university function. Privileges should be assigned on a "least privilege" basis. System owners should regularly review access rights and privileges to ensure they are still needed; activities of interest include terminations, departmental transfers, or roles changes. Access re-certification should be performed at least annually.	
UO.PR.17	**User Access Control: Authentication**	***Authentication shall be required for all access to the system.*** Acceptable UO authentication elements include username/password, PINs, digital certificates, and biometrics. ISO approved authentication sources include one of the following secure/encrypted log-on procedures: Active Directory, LDAP, UO Single Sign-on, external vendor authentication approved by ISO.	
UO.PR.18	**User Access Control: Limit Failed Login Attempts**	***System shall be configured or otherwise controlled to limit failed login attempts to 10 or less, by temporarily disabling the account.***	

		Login attempts should be limited to prevent brute force attacks, where automated tools are used to continuously guess the password until they are successful. Non-privileged accounts may automatically be reenabled after being disabled for 15 - 30 minutes.	
UO.PR.19	**User Access Control: Inactive Session Timeout**	***Controls shall be implemented to timeout or expire sessions after a period of 10 hours or less of inactivity.*** Inactive session timeout reduces exposure to session hijacking attacks, where an attacker could intercept an active session to gain unauthorized access to the system as the user.	
UO.PR.20	**User Access Control: Two-Factor Authentication**	***Two-factor Authentication shall be used, at least once, in the path required for all network access, and for all access by privileged accounts.*** Two-factor authentication refers to the combination of any two of the following factors: 1) ***something you know*** (e.g., a password or PIN), 2) ***something you have*** (e.g., a phone, a token, proximity access card, a digital certificate), 3) ***something you are*** (e.g., finger print, hand scan, iris scan, etc.).	
UO.PR.21	**User Access Control: Remote Privileged Access Session Security**	***Encrypted communication protocols shall be used for remote privileged access to the system.*** Encryption protocols are required for privileged access to the system from outside of the UO wired network (including from the University wireless networks.) Acceptable protocols include SSH, SCP, sFTP, or virtual private network tunneling protocols (TLS or IPSEC VPN). Depending on specific requirements, *split tunneling* may be prohibited to prevent access to the local network and VPN destination network simultaneously.	
UO.PR.22	**Web Reputation Filtering**	***Web Reputation Filtering shall be used to protect user from known malicious websites as identified by ISO.*** Web reputation filtering service tracks known malicious websites to protect users. Web reputation filtering services may be included as part of web browsers or as part of other endpoint protection service. Automatic updating of the blocklist is highly recommended.	
DETECTION Controls			
UO.DE.1	**Logging and Retention**	***System shall be configured to log and retain privileged and non-privileged user activities, and system security events.***	

		Logs should be configured to capture events showing "who did what and when". Systems Logs should be sent to the ISO-approved Logging and Monitoring service to ensure appropriate retention and analysis for security events.	
UO.DE.2	**Log Monitoring**	***System generated logs of user activity and system security events shall be monitored for potential security issues by the system administrator and ISO.*** Logs should be sent to the ISO-approved Logging and Monitoring service to be analyzed for indicators of security issues and to provide alerting and notification.	
UO.DE.3	**File Integrity Monitoring**	***File integrity monitoring shall be used to validate the integrity of important operating system and application software files.*** Unauthorized changes or replacement of critical operating system or application files often signals infiltration by attackers. File integrity monitoring provides a means to detect such changes by using cryptographic methods (e.g. hashing functions) for detection.	
RECOVERY Controls			
UO.RC.1	**Incident Recovery: Backup & Recovery**	***System and data shall be backed up and retained according to University record retention policies, and system owner recovery point and recovery time objectives (RPO, RTO)***. System and data backups should be stored as far away from the original system as possible to avoid destruction of both originals and backups. This is also a key control to recover from dangerous attacks such as ransomware. For desktop computers, users should focus on ensuring that important data is backed up, as opposed to full backup of those systems.	
UO.RC.2	**Incident Recovery: Restoration Testing**	***Backup system shall be tested periodically to verify the integrity of the backup process and recoverability of data and system.*** Recovery testing increase assurance that the process is working correctly and increases confidence that backups are being captured appropriately. This activity can either be done on a scheduled basis or recoveries performed during normal operations can be documented and leveraged as evidence of process and data integrity.	

Acronyms

UNIVERSITY OF OREGON

Information Security Office:
infosec@uoregon.edu
(541) 346-5837

SCCM – Microsoft System Center Configuration Manager

CMDB – Configuration Management Database

SSH – Secure Socket Layer protocol

BYOD – Bring your own device

SCP - Secure Copy protocol

SFTP - Secure File Transfer Protocol

VPN – Virtual Private Network

TLS - Transport Layer Security

IPSec – Internet Protocol Security

SIEM – Security Information and Event Management

CVSS – Common Vulnerability Scoring System, supported by the National Institute of Standards and Technology National Vulnerability Database (NIST NVD)