CIS Ctrl / Sub-Ctrl	Asset Type	Security Function	Title	Description	Responsible	UVA Policy, Standard or Procedure (PSP)	UVA Safeguard or Countermeasure	Control & Framework Reference	Implementation Group 1	Implementation Group 2	Implementation Group 3
1			**Inventory and Control of Hardware Assets**	***Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.***				ISO 27002-2013: A.8.1.1 Inventory of Assets CSC version 7: Controls #1			
1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	UVA InfoSec	No PSP	Axonius			X	X
1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	UVA InfoSec	No PSP	Axonius				X
1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	ITS (central)/Network Administrators (distributed)	No PSP				X	X
1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	LSP/Endpoint Manager	Information Security (IRM-004) policy & Information Security Risk Management Standard requires completing IS-RM			X	X	X
1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	LSP/Endpoint Manager	Security of Connected Devices Standard includes definition of inventory elements.				X	X
1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.	UVA InfoSec/ITS	No PSP			X	X	X
1.7	Devices	Protect	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	UVA InfoSec/ITS Networking	No PSP				X	X
1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	ITS	No PSP	Recommendation to use MSN in UDPS Required for HSVPN access to HSD.				X
2			**Inventory and Control of Software Assets**	***Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.***				ISO 27002-2013: A.12.5.1 Installation of software on operational systems. CSC version 7: Control #2			
2.1	Applications	Identify	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	LSP/Endpoint Manager	No PSP			X	X	X
2.2	Applications	Identify	Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	LSP/Endpoint Manager	No PSP			X	X	X
2.3	Applications	Identify	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.	LSP/Endpoint Manager	No PSP				X	X
2.4	Applications	Identify	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.	LSP/Endpoint Manager	No PSP				X	X
2.5	Applications	Identify	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.	LSP/Endpoint Manager	No PSP					X
2.6	Applications	Respond	Address unapproved software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	LSP/Endpoint Manager	No PSP			X	X	X
2.7	Applications	Protect	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.	LSP/Endpoint Manager	Administrative Privileges on University Endpoints Procedure-Section 2: Granting Administrative Privileges					X
2.8	Applications	Protect	Implement Application Whitelisting of Libraries	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.	LSP/Endpoint Manager	No PSP					X
2.9	Applications	Protect	Implement Application Whitelisting of Scripts	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system.	LSP/Endpoint Manager	No PSP					X
2.10	Applications	Protect	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incurs higher risk for the organization.	LSP/Endpoint Manager	No PSP	HSVPN for network access Security zones (HSZ, SSZ) used to segregate server and strorage devices.				X
3			**Continuous Vulnerabil**	***Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.***				ISO 27002-2013: A.12.6.1 Management of technical vulnerabilities CSC version 7: Control #3			
3.1	Applications	Detect	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	UVA InfoSec/System Managers	Partial - Security of Connected Devices Standard does not include devices that cannot run an agent				X	X
3.2	Applications	Detect	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.	LSP/Endpoint Manager	Security of Connected Devices Standard				X	X
3.3	Users	Protect	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.	UVA InfoSec/LSP/Endpoint Manager	Security of Connected Devices Standard				X	X
3.4	Applications	Protect	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	LSP/Endpoint Manager	University Data Protection Standards-Section 2H Security of Connected Devices Standard-Section 2 Partial - automation not required			X	X	X
3.5	Applications	Protect	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	LSP/Endpoint Manager	Security of Connected Devices Standard-Section 2 Partial - automation not required			X	X	X
3.6	Applications	Respond	Compare Back-to-Back Vulnerability Scans	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	LSP/Endpoint Manager	University Data Protection Standards-Section 2H Security of Connected Devices Standard				X	X
3.7	Applications	Respond	Utilize a Risk-Rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	LSP/Endpoint Manager	Security of Connected Devices Standard				X	X
4			**Controlled Use of Administrative Privileges**	***The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.***				ISO 27002-2013: A.9.1.1 Access control policy CSC version 7: Controls #4, 14, 16			
4.1	Users	Detect	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	Endpoint Manager/System Manager	Administrative Privileges on University Endpoints Procedure Partial - Inventory Of Accounts With Administrative Privileges				X	X
4.2	Users	Protect	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	Endpoint Manager/System Manager	Security of Connected Devices Standard-Section 2; Authentication Standard			X	X	X

CIS Ctrl / Sub-Ctrl	Asset Type	Security Function	Title	Description	Responsible	UVA Policy, Standard or Procedure (PSP)	UVA Safeguard or Countermeasure	Control & Framework Reference	Implementation Group 1	Implementation Group 2	Implementation Group 3
4.3	Users	Protect	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	Endpoint Manager/System Manager	Partial - Authentication Standard-Section2:Minimum Requirements For Endpoint And Account Access: Notes			x	x	x
4.4	Users	Protect	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	Endpoint Manager/System Manager	Authentication Standard-Section 2				X	X
4.5	Users	Protect	Use Multi-Factor Authentication for All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.	Endpoint Manager/System Manager	Authentication Standard-Section 2				X	X
4.6	Users	Protect	Use Dedicated Workstat	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.	Endpoint Manager/System Manager	No PSP					X
4.7	Users	Protect	Limit Access to Script Tools	Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.	Endpoint Manager/System Manager	No PSP				X	X
4.8	Users	Detect	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	Endpoint Manager/System Manager	No PSP				X	X
4.9	Users	Detect	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	Endpoint Manager/System Manager	No PSP				X	X
5			**Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**	***Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.***				ISO 27002-2013 A.14.2.8 System Security Testing CSC version 7: Controls #3, 5, 7, 18, 20			
5.1	Applications	Protect	Establish Secure Configurations	Maintain documented security configuration standards for all authorized operating systems and software.	UVA InfoSec	No PSP			X	X	X
5.2	Applications	Protect	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.	Endpoint Manager/System Manager	No PSP				X	X
5.3	Applications	Protect	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.	Endpoint Manager/System Manager	No PSP				X	X
5.4	Applications	Protect	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.	Endpoint Manager/System Manager	No PSP				X	X
5.5	Applications	Detect	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.	UVA InfoSec	No PSP				X	X
6			**Maintenance, Monitoring and Analysis of Audit Logs**	***Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.***				ISO 27002-2013: A.12.4.1 Event logging CSC version 7: Controls #6, 12, 15			
6.1	Network	Detect	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.	Endpoint Manager/System Manager	No PSP				X	X
6.2	Network	Detect	Activate Audit Logging	Ensure that local logging has been enabled on all systems and networking devices.	Endpoint Manager/System Manager	Partial - University Data Protection Standards-Section 2H Server Access Permissions and Security of Connected Devices Standard	Enterprise Logging Service (Splunk)		X	X	X
6.3	Network	Detect	Enable Detailed Logging	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	Endpoint Manager/System Manager	No PSP	Enterprise Logging Service (Splunk)			X	X
6.4	Network	Detect	Ensure Adequate Storage for Logs	Ensure that all systems that store logs have adequate storage space for the logs generated.	Endpoint Manager/System Manager	No PSP	Enterprise Logging Service (Splunk)			X	X
6.5	Network	Detect	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	Endpoint Manager/System Manager	No PSP	Enterprise Logging Service (Splunk)			X	X
6.6	Network	Detect	Deploy SIEM or Log Analytic Tools	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	Endpoint Manager/System Manager	No PSP	Enterprise Logging Service (Splunk)			X	X
6.7	Network	Detect	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.	Endpoint Manager/System Manager	University Data Protection Standards-Section 2H Server Access Permissions	Enterprise Logging Service (Splunk)			X	X
6.8	Network	Detect	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	Endpoint Manager/System Manager	No PSP	Enterprise Logging Service (Splunk)				X
7			**Email and Web Browse**	***Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.***				ISO 27002-2013 A.14.2.8 System Security Testing CSC version 7: Controls #3, 5, 7, 18, 20			
7.1	Applications	Protect	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	Endpoint Manager/Server Manager; ITS for fully supported browser requirements	Partial - Security of Connected Devices Standard-Section 2			X	X	X
7.2	Applications	Protect	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	Endpoint Manager	No PSP				X	X
7.3	Applications	Protect	Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.	Endpoint Manager	No PSP				X	X
7.4	Network	Protect	Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	UVA InfoSec	No PSP	Partial - Efficient IP on UVA networks			X	X

CIS Ctrl / Sub-Ctrl	Asset Type	Security Function	Title	Description	Responsible	UVA Policy, Standard or Procedure (PSP)	UVA Safeguard or Countermeasure	Control & Framework Reference	Implementation Group 1	Implementation Group 2	Implementation Group 3
7.5	Network	Protect	Subscribe to URL-Categorization Service	Subscribe to URL-categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.	UVA InfoSec	No PSP				X	X
7.6	Network	Detect	Log All URL requester	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.	UVA InfoSec	No PSP				X	X
7.7	Network	Protect	Use of DNS Filtering Services	Use Domain Name System (DNS) filtering services to help block access to known malicious domains.	DNS Administrators	No PSP	Automated Network Blocking		X	X	X
7.8	Network	Protect	Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail(DKIM) standards.	Email Administrators	Security of Connected Devices Standard				X	X
7.9	Network	Protect	Block Unnecessary File Types	Block all email attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.	Email Administrators	No PSP				X	X
7.10	Network	Protect	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.	Email Administrators	No PSP	Microsoft scanning				X
8			**Malware Defenses**	***Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.***				ISO 27002-2013: A.8.3.1 Management of removable media CSC version 7: Controls #8, 13-14			
8.1	Devices	Protect	Utilize Centrally Managed Anti-malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	LSP/Endpoint Manager/ITS	University Data Protection Standards-Section 2H & I (Scanning)				X	X
8.2	Devices	Protect	Ensure Anti-Malware Software and Signatures Are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	LSP/Endpoint Manager/ITS	University Data Protection Standards-Section 2H & I (Scanning)			X	X	X
8.3	Devices	Protect	Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.	LSP/Endpoint Manager	No PSP				X	X
8.4	Devices	Detect	Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	LSP/Endpoint Manager	No PSP			X	X	X
8.5	Devices	Protect	Configure Devices to Not Auto-Run Content	Configure devices to not auto-run content from removable media.	LSP/Endpoint Manager	No PSP			X	X	X
8.6	Devices	Detect	Centralize Anti-Malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	Endpoint Manager/System Manager/	No PSP	Partial - Microsoft Defender for Endpoints users			X	X
8.7	Network	Detect	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	DNS Administrators	No PSP				X	X
8.8	Devices	Detect	Enable Command-Line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.	Endpoint Manager/System Manager	No PSP				X	X
9			**Limitation and Control of Network Ports, Protocols, and Services**	***Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.***				ISO 27002-2013: A.9.1.2 Access to networks and network services CSC version 7: Controls #1, 9, 11-12			
9.1	Devices	Identify	Associate Active Ports, Services, and Protocols to Asset Inventory	Associate active ports, services, and protocols to the hardware assets in the asset inventory.	ITS	No PSP				X	X
9.2	Devices	Protect	Ensure Only Approved Ports, Protocols, and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.	Endpoint Manager/System Manager	No PSP				X	X
9.3	Devices	Detect	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.	UVA InfoSec	No PSP				X	X
9.4	Devices	Protect	Apply Host-Based Firewalls or Port-Filtering	Apply host-based firewalls or port-filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Endpoint Manager/System Manager	Partial - Security of Connected Devices Standard			X	X	X
9.5	Devices	Protect	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	Endpoint Manager/System Manager	Partial - Security of Connected Devices Standard					X
10			**Data Recovery Capabilities**	***The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.***				ISO 27002-2013: A.10.1.1 Policy on the use of cryptographic controls CSC Control #10, 13-15			
10.1	Data	Protect	Ensure Regular Automated Backups	Ensure that all system data is automatically backed up on a regular basis.	Endpoint Manager/System Manager	University Data Protection Standards-Section 2H Shared Devices (Recovery and Physical Security)			X	X	X
10.2	Data	Protect	Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	Endpoint Manager/System Manager	No PSP			X	X	X
10.3	Data	Protect	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	Endpoint Manager/System Manager	No PSP				X	X
10.4	Data	Protect	Protect Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	Endpoint Manager/System Manager	University Data Protection Standards-Section 2F (Via Other Electronic Transmissions)			X	X	X
10.5	Data	Protect	Ensure All Backups Have at Least One Offline Backup Destination	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.	Endpoint Manager/System Manager	No PSP			X	X	X
11			**Secure Configuration for Network Devices, such as Firewalls, Routers and Switches**	***Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.***				ISO 27002-2013: A.9.1.2 Access to networks and network services CSC version 7: Controls #1, 9, 11-12			

CIS Ctrl / Sub-Ctrl	Asset Type	Security Function	Title	Description	Responsible	UVA Policy, Standard or Procedure (PSP)	UVA Safeguard or Countermeasure	Control & Framework Reference	Implementation Group 1	Implementation Group 2	Implementation Group 3
11.1	Network	Identify	Maintain Standard Security Configurations for Network Devices	Maintain documented security configuration standards for all authorized network devices.	Network Administrators	No PSP				X	X
11.2	Network	Identify	Document Traffic Configuration Rules	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.	Network Administrators	No PSP				X	X
11.3	Network	Detect	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configuration against approved security configurations defined for each network device in use, and alert when any deviations are discovered.	Network Administrators	No PSP				X	X
11.4	Network	Protect	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.	Network Administrators	Security of Connected Devices Standard			X	X	X
11.5	Network	Protect	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.	Network Administrators	Authentication Standard				X	X
11.6	Network	Protect	Use Dedicated Machines For All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.	Network Administrators	No PSP				X	X
11.7	Network	Protect	Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	Network Administrators	No PSP				X	X
12			**Boundary Defense**	***Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.***				ISO 27002-2013: A.9.1.2 Access to networks and network services CSC version 7: Controls #1, 9, 11-12			
12.1	Network	Identify	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.	ITS	No PSP			X	X	X
12.2	Network	Detect	Scan for Unauthorized Connections Across Trusted Network Boundaries	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.	UVA InfoSec	No PSP				X	X
12.3	Network	Protect	Deny Communications With Known Malicious IP Addresses	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.	UVA InfoSec/ITS	No PSP	Automated Network Blocking and DNS Blocking			X	X
12.4	Network	Protect	Deny Communication Over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	Network Administrators	No PSP	List of blocked ports: https://in.virginia.edu/blocked-ports		X	X	X
12.5	Network	Detect	Configure Monitoring Systems to Record Network Packets	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	UVA InfoSec	No PSP	Corelight			X	X
12.6	Network	Detect	Deploy Network-Based IDS Sensors	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	UVA InfoSec/Network Administrators	No PSP	FireEye			X	X
12.7	Network	Protect	Deploy Network-Based Intrusion Prevention Systems	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.	UVA InfoSec/Network Administrators	No PSP	https://in.virginia.edu/ips				X
12.8	Network	Detect	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.	UVA InfoSec/Network Administrators	No PSP				X	X
12.9	Network	Detect	Deploy Application Layer Filtering Proxy Server	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.	UVA InfoSec/Network Administrators	No PSP					X
12.10	Network	Detect	Decrypt Network Traffic at Proxy	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	UVA InfoSec/Network Administrators	No PSP					X
12.11	Users	Protect	Require All Remote Login to Use Multi-Factor Authentication	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.	Endpoint Manager/System Manager	Partial - University Data Protection Standards-Section 2F (HSD; Via Other Electronic Transmissions) & Security of Connected Devices Standard				X	X
12.12	Devices	Protect	Manage All Devices Remotely Logging into Internal Network	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	UVA InfoSec/Network Administrators	Partial - Protection of Highly Sensitive Data Standard	Opswat for HS				X
13			**Data Protection**	***The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.***				ISO 27002-2013: A.8.3.1 Management of removable media CSC version 7: Controls #8, 13-14			
13.1	Data	Identify	Maintain an Inventory of Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.	ITS/System Manager/Data Steward	University Data Protection Standards-Section 2F (Responsibility for the Data) Information Security Risk Management Standard			X	X	X
13.2	Data	Protect	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	System Manager	No PSP			X	X	X
13.3	Data	Detect	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	UVA InfoSec/ITS	Partia - Security of Connected Devices Standard					X

CIS Ctrl / Sub-Ctrl	Asset Type	Security Function	Title	Description	Responsible	UVA Policy, Standard or Procedure (PSP)	UVA Safeguard or Countermeasure	Control & Framework Reference	Implementation Group 1	Implementation Group 2	Implementation Group 3
13.4	Data	Protect	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.	System Manager/Data Steward/Unit Heads	Partial - University Data Protection Standards-Section 2G (Storage in General Purpose Electronic File and Workspaces) [Not Email] Vendor Security Review Standard				X	X
13.5	Data	Detect	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.	UVA InfoSec/ITS	No PSP					X
13.6	Data	Protect	Encrypt Mobile Device Data	Utilize approved cryptographic mechanisms to protect enterprise data stored on all mobile devices.	UVA InfoSec/ITS	No PSP			X	X	X
13.7	Data	Protect	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.	UVA InfoSec/ITS	No PSP				X	X
13.8	Data	Protect	Manage System's External Removable Media's Read/Write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.	Endpoint Manager	No PSP					X
13.9	Data	Protect	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.	UVA InfoSec/Data Steward	Partial - For HSD:University Data Protection Standards-Section 2F and 2G					X
14			**Controlled Access Based on the Need to Know**	***The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.***				ISO 27002-2013: A.8.3.1 Management of removable media CSC version 7: Controls #8, 13-14			
14.1	Network	Protect	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).	UVA InfoSec/Network Administrators/Data Steward	No PSP	HSZ and SSZ			X	X
14.2	Network	Protect	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	Network Administrators	No PSP	Networks performs FW filtering			X	X
14.3	Network	Protect	Disable Workstation to Workstation Communication	Disable all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or micro segmentation.	UVA InfoSec/Network Administrators	No PSP				X	X
14.4	Data	Protect	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.	Endpoint Manager/System Manager	University Data Protection Standards-Section 2F				X	X
14.5	Data	Detect	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.	Endpoint Manager/System Manager	Partial - Security of Connected Devices Standard - Email Server; MS Tools					X
14.6	Data	Protect	Protect Information Through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	Endpoint Manager/System Manager	Protection of Highly Sensitive Data Standard			X	X	X
14.7	Data	Protect	Enforce Access Control to Data Through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.	Endpoint Manager/System Manager/UVA InfoSec	Partial - Security of Connected Devices Standard - Email Server; MS Tools					X
14.8	Data	Protect	Encrypt Sensitive Information at Rest	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	Endpoint Manager/System Manager	No PSP					X
14.9	Data	Detect	Enforce Detail Logging for Access or Changes to Sensitive Data	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	Endpoint Manager/System Manager	No PSP					X
15			**Wireless Access Control**	***The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.***				ISO 27002-2013: A.10.1.1 Policy on the use of cryptographic controls CSC Control #10, 13-15			
15.1	Network	Identify	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.	ITS Network Administrators	No PSP				X	X
15.2	Network	Detect	Detect Wireless Access Points Connected to the Wired Network	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	ITS Network Administrators	No PSP				X	X
15.3	Network	Detect	Use a Wireless Intrusion Detection System	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.	ITS Network Administrators	No PSP				X	X
15.4	Devices	Protect	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.	Endpoint Manager/System Manager	Connecting Networking Equipment Standard					X
15.5	Devices	Protect	Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.	Endpoint Manager/System Manager	No PSP					X
15.6	Devices	Protect	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.	Endpoint Manager/System Manager	No PSP				X	X
15.7	Network	Protect	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	ITS Network Administrators	No PSP	Leveraged on networks other than Wahoo, UVA WiFi Setup, UVA Guest.		X	X	X
15.8	Network	Protect	Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which requires mutual, multi-factor authentication.	ITS Network Administrators	No PSP	Leveraged on networks other than Wahoo, UVA WiFi Setup, UVA Guest.				X
15.9	Devices	Protect	Disable Wireless Peripheral Access of Devices	Disable wireless peripheral access of devices [such as Bluetooth and Near Field Communication (NFC)], unless such access is required for a business purpose.	Endpoint Manager/System Manager	No PSP				X	X

CIS Ctrl / Sub-Ctrl	Asset Type	Security Function	Title	Description	Responsible	UVA Policy, Standard or Procedure (PSP)	UVA Safeguard or Countermeasure	Control & Framework Reference	Implementation Group 1	Implementation Group 2	Implementation Group 3
15.10	Network	Protect	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.	ITS Network Administrators	No PSP			X	X	X
16			**Account Monitoring and Control**	***Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.***				ISO 27002-2013: A.9.1.1 Access control policy CSC version 7: Controls #4, 14, 16			
16.1	Users	Identify	Maintain an Inventory of Authentication Systems	Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.	UVA InfoSec	No PSP				X	X
16.2	Users	Protect	Configure Centralized Point of Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.	System Manager	Accounts Provisioning and Deprovisioning Standard-Section 2b				X	X
16.3	Users	Protect	Require Multi-Factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.	Endpoint Manager/System Manager	Partial - Authentication Standard				X	X
16.4	Users	Protect	Encrypt or Hash all Authentication Credentials	Encrypt or hash with a salt all authentication credentials when stored.	Endpoint Manager/System Manager	IRM-003 Data Protection of University Information (passwords are HSD).				X	X
16.5	Users	Protect	Encrypt Transmittal of Username and Authentication Credentials	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	Endpoint Manager/System Manager	University Data Protection Standard-Section 2F				X	X
16.6	Users	Identify	Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.	System Manager or Authentication Manager	No PSP				X	X
16.7	Users	Protect	Establish Process for Revoking Access	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	System Manager or Authentication Manager	Partial - Accounts Provisioning and Deprovisioning Standard				X	X
16.8	Users	Respond	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.	System Manager or Authentication Manager	No PSP			X	X	X
16.9	Users	Respond	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.	System Manager or Authentication Manager	Partial - Accounts Provisioning and Deprovisioning Standard-Section 2b			X	X	X
16.10	Users	Protect	Ensure All Accounts Have An Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.	System Manager or Authentication Manager	No PSP				X	X
16.11	Users	Protect	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.	Endpoint Manager/System Manager	Authentication Standard			X	X	X
16.12	Users	Detect	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.	Endpoint Manager/System Manager/UVA InfoSec	No PSP				X	X
16.13	Users	Detect	Alert on Account Login Behavior Deviation	Alert when users deviate from normal login behavior, such as time-of-day, workstation location, and duration.	Endpoint Manager/System Manager/UVA InfoSec	No PSP					X
17			**Implement a Security Awareness and Training Program**	***For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.***				ISO 27002-2013: A.7.2.2 Information security awareness, education, and training CSC version 7: Control #17			
17.1	N/A	Protect	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviors workforce members are not adhering to, using this information to build a baseline education roadmap.	HR/Data Stewards/System Managers/Department Heads/SME	No PSP				X	X
17.2	N/A	Protect	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behavior.	HR/Data Stewards/System Managers/Department Heads/SME	No PSP				X	X
17.3	N/A	Protect	Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	UVA InfoSec	IRM-002:Acceptable Use of the University's Information Technology Resources			X	X	X
17.4	N/A	Protect	Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards, and business requirements.	UVA InfoSec	No PSP				X	X
17.5	N/A	Protect	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.	UVA InfoSec/System Managers	UDPS-Section 2E			X	X	X
17.6	N/A	Protect	Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.	UVA InfoSec	UDPS-Section 2E			X	X	X
17.7	N/A	Protect	Train Workforce on Sensitive Data Handling	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive information.	Records Management/Deans/Department Heads/UVA InfoSec	UDPS-Section 2E			X	X	X
17.8	N/A	Protect	Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	UVA InfoSec	UDPS-Section 2E			X	X	X
17.9	Users	Protect	Train Workforce Members on Identifying and Reporting Incidents	Train workforce members to be able to identify the most common indicators of an incident and be able to report such an incident.	UVA InfoSec	Reporting an Information Security Incident Procedure			X	X	X
18			**Application Software Security**	***Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.***				ISO 27002-2013: A.14.2.1 Secure development policy CSC version 7: Control #18			
18.1	Applications	Protect	Establish Secure Coding Practices	Establish secure coding practices appropriate to the programming language and development environment being used.	Developers/Unit Heads	No PSP				X	X
18.2	Applications	Protect	Ensure That Explicit Error Checking is Performed for All In-House Developed Software	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.	Developers/Engineers/Unit Heads	No PSP				X	X

CIS Ctrl / Sub-Ctrl	Asset Type	Security Function	Title	Description	Responsible	UVA Policy, Standard or Procedure (PSP)	UVA Safeguard or Countermeasure	Control & Framework Reference	Implementation Group 1	Implementation Group 2	Implementation Group 3
18.3	Applications	Protect	Verify That Acquired Software is Still Supported	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.	Developers/Engineers/Unit Heads	Partial - Security of Connected Devices Standard				X	X
18.4	Applications	Protect	Only Use Up-to-Date and Trusted Third-Party Components	Only use up-to-date and trusted third-party components for the software developed by the organization.	Developers/Engineers/Unit Heads	No PSP					X
18.5	Applications	Protect	Use Only Standardized and Extensively Reviewed Encryption Algorithms	Use only standardized, currently accepted, and extensively reviewed encryption algorithms.	Developers/Engineers/Unit Heads	No PSP				X	X
18.6	Applications	Protect	Ensure Software Development Personnel are Trained in Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.	Unit Heads	No PSP				X	X
18.7	Applications	Protect	Apply Static and Dynamic Code Analysis Tools	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.	Developers/Engineers/Unit Heads	No PSP				X	X
18.8	Applications	Protect	Establish a Process to Accept and Address Reports of Software Vulnerabilities	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.	UVA InfoSec	No PSP	University of Virginia Academic Division Information Security Incident Response Plan abuse@virginia.edu			X	X
18.9	Applications	Protect	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.	Developers/Engineers/Unit Heads	No PSP				X	X
18.10	Applications	Protect	Deploy Web Application Firewalls	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.	Endpoint Manager/System Manager	No PSP				X	X
18.11	Applications	Protect	Use Standard Hardening Configuration Templates for Databases	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.	Developers/Engineers/Unit Heads	Partial - University Data Protection Standards-Section 2H for HSD				X	X
19			**Incident Response and**	***Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.***				ISO 27002-2013: A.7.2.1 Management responsibilities CSC version 7: Control #19			
19.1	N/A	Respond	Document Incident Response Procedures	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.	UVA InfoSec	Information Security of University Technology Resources Policy	University of Virginia Academic Division Information Security Incident Response Plan		X	X	X
19.2	N/A	Respond	Assign Job Titles and Duties for Incident Response	Assign job titles and duties for handling computer and network incidents to specific individuals, and ensure tracking and documentation throughout the incident through resolution.	UVA InfoSec	No PSP	University of Virginia Academic Division Information Security Incident Response Plan			X	X
19.3	N/A	Respond	Designate Management Personnel to Support Incident Handling	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.	UVA InfoSec	No PSP	University of Virginia Academic Division Information Security Incident Response Plan		X	X	X
19.4	N/A	Respond	Devise Organization-wide Standards for Reporting Incidents	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	UVA InfoSec	Reporting an Information Security Incident Standard & Procedure				X	X
19.5	N/A	Respond	Maintain Contact Information For Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners.	UVA InfoSec	No PSP	University of Virginia Academic Division Information Security Incident Response Plan		X	X	X
19.6	N/A	Respond	Publish Information Regarding Reporting Computer Anomalies and Incidents	Publish information for all workforce members, regarding reporting computer anomalies and incidents, to the incident handling team. Such information should be included in routine employee awareness activities.	UVA InfoSec	Reporting an Information Security Incident Standard & Procedure	University of Virginia Academic Division Information Security Incident Response Plan		X	X	X
19.7	N/A	Recover	Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident, response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.	UVA InfoSec	No PSP	University of Virginia Academic Division Information Security Incident Response Plan			X	X
19.8	N/A	Recover	Create Incident Scoring and Prioritization Schema	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	UVA InfoSec	No PSP	University of Virginia Academic Division Information Security Incident Response Plan				X
20			**Penetration Tests and Red Team Exercises**	***Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.***				ISO 27002-2013 A.14.2.8 System Security Testing CSC version 7: Controls #3, 5, 7, 18, 20			
20.1	N/A	Identify	Establish a Penetration Testing Program	Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.	UVA InfoSec	No PSP				X	X
20.2	Network	Identify	Conduct Regular External and Internal Penetration Tests	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.	UVA InfoSec	No PSP				X	X
20.3	N/A	Identify	Perform Periodic Red Team Exercises	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.	UVA InfoSec	No PSP					X
20.4	Network	Identify	Include Tests for Presence of Unprotected System Information and Artifacts	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.	UVA InfoSec	No PSP				X	X
20.5	Network	Identify	Create Test Bed for Elements Not Typically Tested in Production	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.	UVA InfoSec	No PSP				X	X
20.6	Network	Identify	Use Vulnerability Scanning and Penetration Testing Tools in Concert	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.	UVA InfoSec	No PSP				X	X

CIS Ctrl / Sub-Ctrl	Asset Type	Security Function	Title	Description	Responsible	UVA Policy, Standard or Procedure (PSP)	UVA Safeguard or Countermeasure	Control & Framework Reference	Implementation Group 1	Implementation Group 2	Implementation Group 3
20.7	Respond	Identify	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards	Wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.	UVA InfoSec	No PSP					X
20.8	Users	Identify	Control and Monitor Accounts Associated with Penetration Testing	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.	UVA InfoSec	No PSP				X	X