Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.

Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware 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.

Ensure that the hardware 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.

Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.

Utilize port level access control, following IEEE 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware inventory data to ensure only authorized devices can connect to the network.

Use client certificates to authenticate hardware assets connecting to the organization's trusted network.

Maintain 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.

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.

Ensure that unauthorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.

Ensure that unauthorized software is blocked from executing on assets.

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized and unmanaged software is found and prevented from installation or execution.

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.

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized and unmanaged software is found and prevented from installation or execution.

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.

Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.

The software inventory system should track the name, version, publisher, and initial date for all software, including operating systems authorized by the organization.

The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.

Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized and unmanaged software is found and prevented from installation or execution.

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized and unmanaged software is found and prevented from installation or execution.

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized and unmanaged software is found and prevented from installation or execution.

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized and unmanaged software is found and prevented from installation or execution.

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized and unmanaged software is found and prevented from installation or execution.

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized and unmanaged software is found and prevented from installation or execution.

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized and unmanaged software is found and prevented from installation or execution.

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized and unmanaged software is found and prevented from installation or execution.

Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized and unmanaged software is found and prevented from installation or execution.
### Security

4.3 **Users**
- **Protec**
  - 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 and not Internet browsing, email, or similar activities.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: Partial - Authentication Standard-Section 2

4.4 **Users**
- **Protec**
  - 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.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: Authorization Standard-Section 2

4.5 **Users**
- **Protec**
  - Use Multi-Factor Authentication for All Administrative Access
  - Use multi-factor authentication and encrypted channels for all administrative account access.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: Authorization Standard-Section 2

4.6 **Users**
- **Protec**
  - Use Dedicated Workstation
  - Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segregated 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.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: No PSP

4.7 **Users**
- **Protec**
  - Limit Access to Scripting 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.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: No PSP

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.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: No PSP

4.9 **Users**
- **Detect**
  - Log and Alert on Unsuccessful Administrative Account Logins
  - Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: No PSP

### 5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

5.1 **Applications**
- **Protec**
  - Establish Secure Configurations
  - Maintain documented security configuration standards for all authorized operating systems and software.
  - **Responsible**: UVA InfSec
  - **UVA Policy, Standard or Procedure (PSP)**: No PSP

5.2 **Applications**
- **Protec**
  - 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 these images or templates.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: No PSP

5.3 **Applications**
- **Protec**
  - Secure 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.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: No PSP

5.4 **Applications**
- **Protec**
  - Deploy System Configuration Management Tools
  - Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: No PSP

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.
  - **Responsible**: UVA InfSec
  - **UVA Policy, Standard or Procedure (PSP)**: No PSP

### 6. Maintenance, Monitoring and Analysis of Audit Logs

6.1 **Network**
- **Detect**
  - Synchronize 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.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: No PSP

6.2 **Network**
- **Detect**
  - Activate Audit Logging
  - Ensure that local logging has been enabled on all systems and networking devices.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: Enterprise Logging Service (Splunk)

6.3 **Network**
- **Detect**
  - Enable Detailed Logging
  - Enable system logging to include detailed information such as a event source, date, user, timestamp, source address, destination addresses, and other useful elements.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: Enterprise Logging Service (Splunk)

6.4 **Network**
- **Detect**
  - Ensure Adequate Storage for Logs
  - Ensure that all systems that store logs have adequate storage space for the logs generated.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: Enterprise Logging Service (Splunk)

6.5 **Network**
- **Detect**
  - Central Log Management
  - Ensure that appropriate logs are being aggregated to a central log management system for analysis.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: Enterprise Logging Service (Splunk)

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.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: Enterprise Logging Service (Splunk)

6.7 **Network**
- **Detect**
  - Regularly Review Logs
  - On a regular basis, review logs to identify anomalies or abnormal events.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: Enterprise Logging Service (Splunk)

6.8 **Network**
- **Detect**
  - Regularly Tune SIEM
  - On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.
  - **Responsible**: Endpoint Manager/System Manager
  - **UVA Policy, Standard or Procedure (PSP)**: Enterprise Logging Service (Splunk)

### 7. Email and Web Browser

7.1 **Applications**
- **Protec**
  - 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.
  - **Responsible**: Endpoint Manager/Server Manager; ITS for fully supported browser requirements
  - **UVA Policy, Standard or Procedure (PSP)**: Partial - Security of Connected Devices Standard-Section 2

7.2 **Applications**
- **Protec**
  - Disable Unnecessary or Unauthorized Browser or Email Client Plugins
  - Uninstall or disable any unauthorized browser or email client plugins or add-on applications.
  - **Responsible**: Endpoint Manager
  - **UVA Policy, Standard or Procedure (PSP)**: No PSP

7.3 **Applications**
- **Protec**
  - 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.
  - **Responsible**: Endpoint Manager
  - **UVA Policy, Standard or Procedure (PSP)**: No PSP

7.4 **Network**
- **Protec**
  - 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.
  - **Responsible**: UVA InfSec
  - **UVA Policy, Standard or Procedure (PSP)**: Partial - Efficient IP on UVA network

---

**Notes**

- **Groups**: Group 1, 2, 3
- **References**: ISO 27001-2013 A.14.2.8
- **Controls**: #3, 5, 7, 16, 20
- **UVA References**: No PSP
- **Implementation**: No PSP

---

**References**

- ISO 27001-2013 A.14.2.8 System Security Testing CSC version 7: Controls #3, 5, 7, 16, 20
<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
<th>Responsible</th>
<th>UVA Policy, Standard or Procedure (PS)</th>
<th>UVA Safeguard or Countermeasure</th>
<th>Control &amp; Framework Reference</th>
<th>Implementation Group 1</th>
<th>Implementation Group 2</th>
<th>Implementation Group 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.5</td>
<td>Network</td>
<td>Network Protect</td>
<td>Subscribe to URL-Categorization Service</td>
<td>UVA InfoSec</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>7.6</td>
<td>Network</td>
<td>Network Protect</td>
<td>Log All URL requests</td>
<td>UVA InfoSec</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>7.7</td>
<td>Network</td>
<td>Network Protect</td>
<td>Use of DNS Filtering Services</td>
<td>DNS Administrators</td>
<td>No PSP</td>
<td>Automated Network Blocking</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>7.8</td>
<td>Network</td>
<td>Network Protect</td>
<td>Use Domain Name System (DNS) filtering services to help block access to known malicious domains.</td>
<td>DNS Administrators</td>
<td>No PSP</td>
<td>Automated Network Blocking</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>7.9</td>
<td>Network</td>
<td>Network Protect</td>
<td>Block Unnecessary File Types</td>
<td>Email Administrators</td>
<td>No PSP</td>
<td>Security of Connected Devices Standard</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>7.10</td>
<td>Network</td>
<td>Network Protect</td>
<td>Send sandboxing to analyze and block inbound email attachments with malicious behavior.</td>
<td>Email Administrators</td>
<td>No PSP</td>
<td>Microsoft scanning</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

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 defenses, data gathering, and corrective action.

8.1 Devices | Devices Protect | Utilize centrally managed anti-malware software | LSP/Endpoint Manager/ITS | University Data Protection Standards-Section 9H & I Scanning | X | X | X |
8.2 Devices | Devices Protect | Ensure that anti-malware software updates its scanning engine and signature database on a regular basis. | LSP/Endpoint Manager/ITS | University Data Protection Standards-Section 9H & I Scanning | X | X | X |
8.3 Devices | Devices Protect | 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 tools that can be configured to apply protection to a broader set of applications and executables. | LSP/Endpoint Manager | No PSP | X | X | X |
8.4 Devices | Devices Protect | 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 | Devices Protect | Configure devices to not auto-run content from removable media. | LSP/Endpoint Manager | No PSP | X | X | X |
8.6 Devices | Devices Protect | Centralize Anti-Malware Logging | Endpoint Manager/System Manager | No PSP | Partial - Microsoft Defender for Endpoints users | X | X | X |
8.7 Network | Network Detect | Enable DNS Query Logging | DNS Administrators | No PSP | X | X | X |
8.8 Devices | Devices Detect | Enable Command-Line Audit Logging | Endpoint Manager/System Manager | No PSP | X | X | X |

9  Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/monitor) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

9.1 Devices | Devices Identify | Associate Active Ports, Services, and Protocols to Asset Inventory | ITS | No PSP | X | X | X |
9.2 Devices | Devices Protect | Ensure Only Approved Ports, Protocols, and Services Are Running | Endpoint Manager/System Manager | No PSP | X | X | X |
9.3 Devices | Devices Protect | Perform Regular Automated Port Scans | UVA InfoSec | No PSP | X | X | X |
9.4 Devices | Devices Protect | Apply Host-Based Firewalls or Port-Filing 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 | Devices Protect | Implement Application Firewalls | Endpoint Manager/System Manager | Partial - Security of Connected Devices Standard | X | X | 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.

10.1 Data | Data Protect | Ensure Regular Backups | Endpoint Manager/System Manager | University Data Protection Standards-Section 9H Shared Devices (Recovery and Physical Security) | X | X | X |
10.2 Data | Data Protect | Perform Complete System Backups | Endpoint Manager/System Manager | No PSP | X | X | X |
10.3 Data | Data Protect | Test Data on Backup Media | Endpoint Manager/System Manager | No PSP | X | X | X |
10.4 Data | Data Protect | Protect Backups | Endpoint Manager/System Manager | University Data Protection Standards-Section 2F (Via Other Electronic Transmissions) | X | X | X |
10.5 Data | Data Protect | Ensure All Backups Have at Least One Offline 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.

11.1 Secure Configuration | 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 A7.9.11-12 | X | X | X |

ISO 27002-2013: A.3.3.1 Management of removable media CSC version 7. Controls A7.9.11-12 | X | X | X |

<table>
<thead>
<tr>
<th>CSC Code</th>
<th>Sub-Code</th>
<th>Asset Type</th>
<th>Security Function</th>
<th>Description</th>
<th>Responsible</th>
<th>UVA Policy, Standard or Procedure (PSP)</th>
<th>UVA Safeguard or Countermeasure</th>
<th>Control &amp; Framework Reference</th>
<th>Implementation Group 1</th>
<th>Implementation Group 2</th>
<th>Implementation Group 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td></td>
<td>Network</td>
<td>Identify</td>
<td>Maintain Security Configurations for Network Devices</td>
<td>Network Administrators</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.2</td>
<td></td>
<td>Network</td>
<td>Identify</td>
<td>Document Traffic Configuration Rules</td>
<td>Network Administrators</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.3</td>
<td></td>
<td>Network</td>
<td>Detect</td>
<td>Use Automated Tools to Verify Standard Device Configurations and Detect Changes</td>
<td>Network Administrators</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.5</td>
<td></td>
<td>Network</td>
<td>Protect</td>
<td>Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions</td>
<td>Network Administrators</td>
<td>Authentication Standard</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.6</td>
<td></td>
<td>Network</td>
<td>Protect</td>
<td>Use Dedicated Machine For All Network Administrators Tasks</td>
<td>Network Administrators</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.7</td>
<td></td>
<td>Network</td>
<td>Protect</td>
<td>Manage Network Infrastructure Through a Dedicated Network</td>
<td>Network Administrators</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>Boundary Defense</td>
<td>Detect/prevent/conflict the flow of information transferring networks of different trust levels with a focus on security-damaging data.</td>
<td></td>
<td>ISO 27002-2013: A.3.1.2 Access to networks and network services CSC version 7 Controls 41, 9, 11-12</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.1</td>
<td></td>
<td>Network</td>
<td>Identify</td>
<td>Maintain an Inventory of Network Boundaries</td>
<td>ITS</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.2</td>
<td></td>
<td>Network</td>
<td>Detect</td>
<td>Scan for Unauthorized Connections Across Trusted Network Boundaries</td>
<td>UVA InfoSec</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.3</td>
<td></td>
<td>Network</td>
<td>Protect</td>
<td>Deny Communications From Known Malicious IP Addresses</td>
<td>UVA InfoSec/ITS</td>
<td>Automated Network Blocking and DNS Blocking</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.4</td>
<td></td>
<td>Network</td>
<td>Protect</td>
<td>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.</td>
<td>Network Administrators</td>
<td>List of blocked ports</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.5</td>
<td></td>
<td>Network</td>
<td>Detect</td>
<td>Configure Monitoring Systems to Record Network Packets Passing through the boundary at each of the organization's network boundaries.</td>
<td>UVA InfoSec</td>
<td>Corelight</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.6</td>
<td></td>
<td>Network</td>
<td>Protect</td>
<td>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.</td>
<td>UVA InfoSec/Network Administrators</td>
<td>FireEye</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.7</td>
<td></td>
<td>Network</td>
<td>Protect</td>
<td>Deploy Network-Based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.</td>
<td>UVA InfoSec/Network Administrators</td>
<td><a href="https://in.virginia.edu/ips">https://in.virginia.edu/ips</a></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.8</td>
<td></td>
<td>Network</td>
<td>Protect</td>
<td>Deploy NetFlow Collection on Networking Boundary Devices</td>
<td>UVA InfoSec/Network Administrators</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.9</td>
<td></td>
<td>Network</td>
<td>Protect</td>
<td>Deploy Application Layer Filtering Proxy Server</td>
<td>UVA InfoSec/Network Administrators</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.10</td>
<td></td>
<td>Network</td>
<td>Protect</td>
<td>Decrypt any encrypted network traffic at the boundary prior to analyzing the content. However, the organization may choose to allow traffic to be decrypted through the proxy without encrypting the traffic.</td>
<td>UVA InfoSec/Network Administrators</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.11</td>
<td></td>
<td>Users</td>
<td>Protect</td>
<td>Require All Remote Login to Use Multi-Factor Authentication</td>
<td>Endpoint Manager/System Manager</td>
<td>Partial - University Data Protection Standards-Section 2F (HIPD, Via Other Electronic Transmissions) &amp; Security of Connected Devices Standard</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.12</td>
<td></td>
<td>Devices</td>
<td>Protect</td>
<td>Manage All Devices Remotely Logging into Internal Network</td>
<td>UVA InfoSec/Network Administrators</td>
<td>Partial - Protection of Sensitive Data Standard</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>Data Protection</td>
<td>The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.</td>
<td></td>
<td>ISO 27002-2013: A.8.3.1 Management of removable media CSC version 7 Controls 41, 9, 13-14</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.1</td>
<td></td>
<td>Data</td>
<td>Identify</td>
<td>Maintain an Inventory of Sensitive Information</td>
<td>ITS/System Manager/Data Steward</td>
<td>University Data Protection Standards-Section 2F (Responsibility for the Data) Information Security Risk Management Standard</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13.2</td>
<td></td>
<td>Data</td>
<td>Protect</td>
<td>Remove Sensitive Data from Systems Not Regularly Accessed by Organization</td>
<td>System Manager</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISG Ctrl</td>
<td>Sub-Cell</td>
<td>Asset Type</td>
<td>Security Function</td>
<td>Title</td>
<td>Description</td>
<td>Responsible</td>
<td>UVA Policy, Standard or Procedure (PSP)</td>
<td>UVA Safeguard or Countermeasure</td>
<td>Control &amp; Framework Reference</td>
<td>Implementation Group 1</td>
<td>Implementation Group 2</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>------------</td>
<td>------------------</td>
<td>-------</td>
<td>-------------</td>
<td>-------------</td>
<td>----------------------------------</td>
<td>---------------------------------</td>
<td>--------------------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>14.1</td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
<td>Segment the Network</td>
<td>Based on Sensitive</td>
<td>Segment the network based on the label or classification level of the information stored on the servers, locations all sensitive information on separated Virtual Local Area Networks (VLANs)</td>
<td>UVA InfoSec/Network Administrators/Data Steward</td>
<td>No PSP</td>
<td>NSIS and NSZ</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>14.2</td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
<td>Enable Firewall Filtering Between VLANs</td>
<td>Enables firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities</td>
<td>Network Administrators</td>
<td>No PSP</td>
<td>Networks performs FW filtering</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>14.3</td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
<td>Disable Workstation to Workstation Communication</td>
<td>Disable all workstation-to-workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, by using technologies such as Private VLANs or microsegmentation</td>
<td>UVA InfoSec/Network Administrators</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.4</td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td>Encrypt All Sensitive Information in Transit</td>
<td>Encrypt all sensitive information in transit</td>
<td>Endpoint Manager/System Manager</td>
<td>University Data Protection Standards-Section 2F</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.5</td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td>Protect Information Through Access Control Lists</td>
<td>Protect all information stored on systems with file system, network shares, 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.</td>
<td>Endpoint Manager/System Manager</td>
<td>Partial - Security of Connected Devices Standard - Email Server, MS Tools</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.6</td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td>Enforce Access Controls to Data Through Automated Tools</td>
<td>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</td>
<td>Endpoint Manager/System Manager/UVA InfoSec</td>
<td>Partial - Security of Connected Devices Standard - Email Server; MS Tools</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.7</td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td>Encrypt Sensitive Information at Rest</td>
<td>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.</td>
<td>Endpoint Manager/System Manager</td>
<td>No PSP</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.8</td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td>Enforce Detailed Logging for Access to Sensitive Data</td>
<td>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).</td>
<td>Endpoint Manager/System Manager</td>
<td>No PSP</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14.9</td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Wireless Access Control</td>
<td>Wireless Access Control</td>
<td>The processes and tools used to track/control/prevent/correct access to critical assets are e.g., information, resources, system(s) 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.</td>
<td>ISO 27002:2013, A.8.3.3 Management of removable media CSC version 7: Controls #13-14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.1</td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
<td>Maintain an Inventory of Authorized Wireless Access Points</td>
<td>Maintain an inventory of authorized wireless access points connected to the wired network.</td>
<td>ITS Network Administrators</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.2</td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
<td>Detect Wireless Access Points Connected to the Wired Network</td>
<td>Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.</td>
<td>ITS Network Administrators</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.3</td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
<td>Use a Wireless Intrusion Detection System</td>
<td>Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.</td>
<td>ITS Network Administrators</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.4</td>
<td>Devices</td>
<td>Devices</td>
<td>Devices</td>
<td>Disable Wireless Access on Devices If Not Required</td>
<td>Disable wireless access on devices that do not have a business purpose for wireless access.</td>
<td>Endpoint Manager/System Manager</td>
<td>Connecting Networking Equipment Standard</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.5</td>
<td>Devices</td>
<td>Devices</td>
<td>Devices</td>
<td>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.</td>
<td>Endpoint Manager/System Manager</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.6</td>
<td>Devices</td>
<td>Devices</td>
<td>Devices</td>
<td>Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients</td>
<td>Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.</td>
<td>Endpoint Manager/System Manager</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.7</td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
<td>Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data</td>
<td>Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.</td>
<td>ITS Network Administrators</td>
<td>No PSP</td>
<td>Leverage on networks other than UVA, UVA WiFi Setup, UVA Guest</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>15.8</td>
<td>Network</td>
<td>Network</td>
<td>Network</td>
<td>Use Wireless Authentication Protocols That Require Mutual, Multi-Factor Authentication</td>
<td>Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), which requires mutual, multi-factor authentication</td>
<td>ITS Network Administrators</td>
<td>No PSP</td>
<td>Leverage on networks other than UVA, UVA WiFi Setup, UVA Guest</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15.9</td>
<td>Devices</td>
<td>Devices</td>
<td>Devices</td>
<td>Disable Wireless Peripheral Access of Devices</td>
<td>Disable wireless peripheral access of devices (such as Bluetooth and Near Field Communication (NFC)), unless such access is required for a business purpose.</td>
<td>Endpoint Manager/System Manager</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
15.10 Network

15.10.1 No PSP

Network

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

ISO 27002:2013: A.9.1.1

Access control policy

Control & Framework Reference

Implementation Group 1

Implementation Group 2

Implementation Group 3

16 Users

16.1 Identify

16.1.1 No PSP

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

16.2 Protect

16.2.1 No PSP

Provision 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 De-provisioning Standard-Section 2b

X

16.3 Protect

16.3.1 No PSP

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

16.4 Protect

16.4.1 No PSP

Encrypt or Hash all Authentication Credentials

Encrypt or hash with a well all authentication credentials when stored.

Endpoint Manager/System Manager

PIA-003 Data Protection of University Information (passwords are not HDI)

X

16.5 Protect

16.5.1 No PSP

Encrypt and Transmit all Usernames 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

16.6 Identify

16.6.1 No PSP

Maintain an Inventory of Accounts

Maintain an inventory of all accounts organized by authentication system.

System Manager or Authentication Manager

No PSP

X

16.7 Protect

16.7.1 No PSP

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 De-provisioning Standard

X

16.8 Respond

16.8.1 No PSP

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

16.9 Respond

16.9.1 No PSP

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

16.10 Protect

16.10.1 No PSP

Lock Workstation Sessions After Inactivity

Automatically lock workstation sessions after a standard period of inactivity.

Endpoint Manager/System Manager

Authorization Standard

X

16.11 Detect

16.11.1 No PSP

Monitor Attempts to Access Deactivated Accounts

Monitor attempts to access deactivated accounts through audit logging.

Endpoint Manager/System Manager

No PSP

X

16.12 Detect

16.12.1 No PSP

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

17.1 N/A

17.1.1 No PSP

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/IT/InfoSec/Univ/Safety/Staff

No PSP

X

17.2 N/A

17.2.1 No PSP

Deliver Training to Fill the Skills Gap

Deliver training to address the skills gap identified to positively impact workforce members’ security behavior.

HR/IT/InfoSec/Univ/Safety/Staff

No PSP

X

17.3 N/A

17.3.1 No PSP

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 secure the safety of the organization. The organization’s security awareness program should be communicated in a concise and engaging manner.

UVA InfoSec

PIA-002 Acceptable Use of the University’s Information Technology Resources

X

17.4 N/A

17.4.1 No PSP

Update Awareness Training 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

17.5 N/A

17.5.1 No PSP

Train Workforce on Secure Authentication

Train workforce members on the importance of enabling and utilizing secure authentication.

UVA InfoSec/Univ/Safety

UDPS-Section 2E

X

17.6 N/A

17.6.1 No PSP

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

17.7 N/A

17.7.1 No PSP

Train Workforce on Sensitive Data Handling

Train workforce members to be aware of and properly store, transfer, archive, and destroy sensitive information.

Records Management/Dean/Dep/Envoy/Head/UVA InfoSec

UDPS-Section 2E

X

17.8 N/A

17.8.1 No PSP

Train Workforce on Causes of Unintentional Data Exposure

Train workforce members to be aware of causes of 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

17.9 N/A

17.9.1 No PSP

Train Workforce on Identifying and Reporting Incident

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

Reporing an Information Security Incident Procedure

X

18 Application Software Security

18.1 Application

18.1.1 No PSP

Establish Secure Coding Practices

Establish secure coding practices appropriate to the programming language and development environment being used.

Developers/Unit Heads

No PSP

X

18.2 Application

18.2.1 No PSP

Establish Secure Coding Practices

Establish secure coding practices appropriate to the programming language and development environment being used.

Developers/Engineers/Un H Heads

No PSP

X
<table>
<thead>
<tr>
<th>CSC Ctrl/ Sub-Cell</th>
<th>Asset Type</th>
<th>Security Function</th>
<th>Title</th>
<th>Description</th>
<th>Responsible</th>
<th>UVA Policy, Standard or Procedure (PSP)</th>
<th>UVA Safeguard or Countermeasure</th>
<th>Control &amp; Framework Reference</th>
<th>Implementation Group 1</th>
<th>Implementation Group 2</th>
<th>Implementation Group 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.3 Applications</td>
<td>Protect</td>
<td>Verify That Acquired Software is Still Supported</td>
<td>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.</td>
<td>Developers/Engineers/IT Heads</td>
<td>Partial - Security of Connected Devices Standard</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.4 Applications</td>
<td>Protect</td>
<td>Only Use Up-to-Date and Trusted Third-Party Components</td>
<td>Only use up-to-date and trusted third-party components for the software developed by the organization.</td>
<td>Developers/Engineers/IT Heads</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.5 Applications</td>
<td>Protect</td>
<td>Use Only Standardized and Extensively Reviewed Encryption Algorithms</td>
<td>Use only standardized, currently accepted, and extensively reviewed encryption algorithms.</td>
<td>Developers/Engineers/IT Heads</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.6 Applications</td>
<td>Protect</td>
<td>Ensure Software Development Personnel are Trained in Secure Coding</td>
<td>Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.</td>
<td>Unit Heads</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.7 Applications</td>
<td>Protect</td>
<td>Apply Static and Dynamic Code Analysis Tools</td>
<td>Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.</td>
<td>Developers/Engineers/IT Heads</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.8 Applications</td>
<td>Protect</td>
<td>Establish a Process to Accept and Address Reports of Software Vulnerabilities</td>
<td>Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.</td>
<td>UVA InfoSec</td>
<td>No PSP</td>
<td>University of Virginia Academic Division Information Security Incident Response Plan <a href="mailto:abuse@virginia.edu">abuse@virginia.edu</a></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.9 Applications</td>
<td>Protect</td>
<td>Separate Production and Non-Production Systems</td>
<td>Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.</td>
<td>Developers/Engineers/IT Heads</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.10 Applications</td>
<td>Protect</td>
<td>Deploy Web Application Firewalls</td>
<td>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.</td>
<td>Endpoint Manager/System Manager</td>
<td>No PSP</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18.11 Applications</td>
<td>Protect</td>
<td>Use Standard Hardening Configuration Templates for Databases</td>
<td>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.</td>
<td>Developers/Engineers/IT Heads</td>
<td>Partial - University Data Protection Standards-Section 4B for HSC</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

19. Incident Response and Red Team Exercises

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.7.2.3 Management responsibilities - CISC version 7: Control A9

| 19.1 N/A Response | N/A | 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 |
| 19.2 N/A Response | N/A | 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 Response | N/A | 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 |
| 19.4 N/A Response | N/A | Develop Organization-wide Standards for Reporting Incidents | Develop 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 Response | N/A | 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 |
| 19.6 N/A Response | N/A | 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 training employee awareness activities. | UVA InfoSec | Reporting an Information Security Incident Standard & Procedure | University of Virginia Academic Division Information Security Incident Response Plan | X | X |
| 19.7 N/A Recovery | N/A | 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 Recovery | N/A | Create Incident Scoring and Prioritization Scheme | 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 | X | University of Virginia Academic Division Information Security Incident Response Plan | X | 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.


<p>| 20.1 N/A Identify | N/A | 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 | N/A | Perform Periodic Host Team Exercises | Perform periodic host team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively. | UVA InfoSec | No PSP | X | X |
| 20.4 Network | Identify | Include Tests for the 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 |</p>
<table>
<thead>
<tr>
<th>Ob. Obj.</th>
<th>Asset Type</th>
<th>Security Function</th>
<th>Title</th>
<th>Description</th>
<th>Responsible</th>
<th>UVA Policy, Standard or Procedure (PSP)</th>
<th>UVA Safeguard or Countermeasure</th>
<th>Control &amp; Framework Reference</th>
<th>Implementation Group 1</th>
<th>Implementation Group 2</th>
<th>Implementation Group 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.7</td>
<td>Respond</td>
<td>Identify</td>
<td>Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards</td>
<td>Whenever 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.</td>
<td>UVA InfoSec</td>
<td>No PSP</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>20.8</td>
<td>Users</td>
<td>Identify</td>
<td>Control and Monitor Accounts Associated with Penetration Testing</td>
<td>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.</td>
<td>UVA InfoSec</td>
<td>No PSP</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>