Minimum Security Standards

Purpose

Virginia Tech is committed to protecting the privacy of its students, alumni, faculty, and current and former employees, as well as protecting the confidentiality, integrity, and availability of information important to the university’s mission.

Scope

These standards are intended to reflect the minimum level of care necessary for Virginia Tech’s data. They do not relieve Virginia Tech or its employees, partners, consultants, or vendors of further obligations that may be imposed by law, regulation or contract. Virginia Tech expects all partners, consultants, and vendors to abide by Virginia Tech's information security policies. If nonpublic information is to be accessed or shared with these third parties, they should be bound by contract to abide by Virginia Tech's information security policies.

Standard

Each of the standards below are mapped to version 8 of the CIS Controls. Prioritize your systems by risk level. As cybersecurity is a rapidly evolving field that continuously presents us with new challenges, these standards will be revised and updated accordingly.

Minimum Security Standards: Endpoints

An endpoint is defined as any laptop, desktop, or mobile device.

Determine the risk level by reviewing the data, server, and application risk classification examples and selecting the highest applicable risk designation across all. For example, an endpoint storing Low Risk Data, but utilized to manage/configure a High Risk application is designated as High Risk.

Follow the minimum security standards in the table below to safeguard your endpoints.

<table>
<thead>
<tr>
<th>STANDARDS</th>
<th>WHAT TO DO</th>
<th>L</th>
<th>M</th>
<th>H</th>
<th>CSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1: Patching</td>
<td>Apply security patches within 30 days of publish. BigFix is recommended. Use a supported OS version.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>7</td>
</tr>
<tr>
<td>E2: Encryption</td>
<td>Meet the Standard for High Risk Digital Data Protection requirements.</td>
<td></td>
<td></td>
<td>✓</td>
<td>3</td>
</tr>
<tr>
<td>E3: Malware Protection</td>
<td>Install antivirus software if possible and configure to automatically update and run scheduled scans.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>10</td>
</tr>
<tr>
<td>E4: Backup</td>
<td>Backup local user data at least weekly. Consider using Network Backup Service.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>11</td>
</tr>
<tr>
<td>E5: Inventory</td>
<td>Register your endpoint with departmental inventory system.</td>
<td></td>
<td></td>
<td>✓</td>
<td>1</td>
</tr>
</tbody>
</table>
### Minimum Security Standards: Servers

A server is defined as a host that provides a network accessible service.

Determine the risk level by reviewing the data, server, and application risk classification examples and selecting the highest applicable risk designation across all. For example, a server running a low risk application, but storing high risk data is designated as High Risk.

Follow the minimum security standards in the table below to safeguard your servers.

<table>
<thead>
<tr>
<th>STANDARD</th>
<th>WHAT TO DO</th>
<th>L</th>
<th>M</th>
<th>H</th>
<th>CSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>E6: Firewall</td>
<td>Enable host-based firewall in default deny mode and permit only the minimum necessary services.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>13</td>
</tr>
<tr>
<td>E7: Equipment Disposal</td>
<td>All university-owned equipment must go through Surplus Property for disposal.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>1</td>
</tr>
<tr>
<td>E8: Credentials and Access Control</td>
<td>Configure workstations and laptops to prohibit anonymous access. Enforce password age, length, and complexity. Require password-protected screen savers, with a recommended 15-minute time for inactivity, or lock device before leaving it unattended.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>5, 6</td>
</tr>
<tr>
<td>E9: Configuration Management</td>
<td>Install BigFix or equivalent (Kaseya)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>4, 7</td>
</tr>
<tr>
<td>E10: Data Security Controls</td>
<td>Implement PCI DSS, FISMA, or export controls as applicable. Meet the Standard for High Risk Digital Data Protection requirements.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>3, 6, 13</td>
</tr>
<tr>
<td>E11: Centralized Logging</td>
<td>Meet the Standard for Information Technology Logging requirements. Forward logs to University Central or ITSO authorized log server. Authorized log servers should provide a feed to the University Central log server.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>8</td>
</tr>
</tbody>
</table>

**STANDARDS**

**WHAT TO DO**

**L** | **M** | **H** | **CSC**

---

**E6: Firewall**

Enable host-based firewall in default deny mode and permit only the minimum necessary services.

**E7: Equipment Disposal**

All university-owned equipment must go through Surplus Property for disposal.

**E8: Credentials and Access Control**

Configure workstations and laptops to prohibit anonymous access. Enforce password age, length, and complexity. Require password-protected screen savers, with a recommended 15-minute time for inactivity, or lock device before leaving it unattended.

**E9: Configuration Management**

Install BigFix or equivalent (Kaseya)

**E10: Data Security Controls**

Implement PCI DSS, FISMA, or export controls as applicable. Meet the Standard for High Risk Digital Data Protection requirements.

**E11: Centralized Logging**

Meet the Standard for Information Technology Logging requirements. Forward logs to University Central or ITSO authorized log server. Authorized log servers should provide a feed to the University Central log server.

---

**S1: Patching**

Based on National Vulnerability Database, apply critical and high severity security patches within seven days of publish and all other security patches within 90 days. Use a supported OS.

**S2: Inventory**

Register your server with departmental inventory system. Send the ITSO a list of department’s high risk servers.
<table>
<thead>
<tr>
<th>STANDARD</th>
<th>WHAT TO DO</th>
<th>L</th>
<th>M</th>
<th>H</th>
<th>CSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3: Firewall</td>
<td>Enable host-based firewall in default deny mode and permit only the minimum necessary services.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>13</td>
</tr>
<tr>
<td>S4: Credentials, Access Control</td>
<td>Review existing accounts and privileges at least annually. Enforce password age, length, and complexity. Configure servers to prohibit anonymous access. Require password-protected screen savers, with a recommended 15-minute time for inactivity, or lock screen before leaving unattended.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>5, 6</td>
</tr>
<tr>
<td>S5: Two-Factor Authentication</td>
<td>Require two-factor authentication for interactive user and administrator logins.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>5</td>
</tr>
<tr>
<td>S6: Equipment Disposal</td>
<td>All university-owned machines must go through Surplus Property for disposal.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>1</td>
</tr>
<tr>
<td>S7: Sysadmin Training</td>
<td>Attend at least one security training course annually.</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>14</td>
</tr>
<tr>
<td>S8: Malware Protection</td>
<td>Use Wazuh, OSSEC or equivalent security monitoring tool. Review alerts as they are received.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>10</td>
</tr>
<tr>
<td>S9: Intrusion Detection</td>
<td>Use Wazuh, OSSEC or equivalent security monitoring tool. Review alerts as they are received.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>13</td>
</tr>
<tr>
<td>S10: Physical Protection</td>
<td>Place system hardware in a data center or controlled access environment.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>1</td>
</tr>
<tr>
<td>S11: Centralized Logging</td>
<td>Meet the Standard for Information Technology Logging requirements. Forward logs to University Central or ITSO authorized log server. Authorized log servers should provide a feed to the University Central log server.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>8</td>
</tr>
<tr>
<td>S12: Security Review</td>
<td>Request a security review and implement recommendations prior to deployment.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
</tr>
<tr>
<td>S13: Vulnerability Management</td>
<td>Perform a quarterly scan. This is a requestable service catalog item. Resolve critical and high vulnerabilities within seven days of the scan.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>6</td>
</tr>
<tr>
<td>S14: Backups</td>
<td>Implement a backup &amp; recovery process sufficient to restore the server to a trusted state. Maintain backups in a separate, offsite environment whenever possible.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>11</td>
</tr>
<tr>
<td>S15: Data Security Controls</td>
<td>Implement PCI DSS, FISMA, or export controls as applicable. Meet the Standard for High Risk Digital Data Protection requirements.</td>
<td></td>
<td></td>
<td>✓</td>
<td>3, 6, 13</td>
</tr>
</tbody>
</table>
Minimum Security Standards: Applications

An application is defined as software running on a server that is remotely accessible, including mobile applications.

Determine the risk level by reviewing the data, server, and application risk classification examples and selecting the highest applicable risk designation across all. For example, an application providing access to low risk data, but running on a high risk server is designated as high risk.

Follow the minimum security standards in the table below to safeguard your applications.

<table>
<thead>
<tr>
<th>STANDARD</th>
<th>WHAT TO DO</th>
<th>L</th>
<th>M</th>
<th>H</th>
<th>CSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1: Patching</td>
<td>Based on National Vulnerability Database, apply critical and high severity security patches within seven days of publish and all other security patches within 90 days. Use a supported version of the application.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>16</td>
</tr>
<tr>
<td>A2: Inventory</td>
<td>Maintain a list of applications and the associated risk classification and data volume estimates. Review and update records quarterly. Send the ITSO a list of department’s high risk applications and their URLs.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>2, 7</td>
</tr>
<tr>
<td>A3: Firewall</td>
<td>Permit the minimum necessary services through the application firewall.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>13,16</td>
</tr>
<tr>
<td>A4: Access Control</td>
<td>Review existing accounts and privileges at least annually. Enforce Virginia Tech Password Rules, Requirements and Tips.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>5, 6</td>
</tr>
<tr>
<td>A5: Two Factor Authentication</td>
<td>Require two-factor authentication for interactive and administrator logins.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>4</td>
</tr>
<tr>
<td>A6: Backups</td>
<td>For high-risk applications, back up application data at least daily. For moderate and low applications, back up data weekly. Encrypt backup data in transit and at rest.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>11</td>
</tr>
<tr>
<td>A7: Developer Training</td>
<td>Attend at least one security training course annually.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>14, 16</td>
</tr>
<tr>
<td>A8: Secure Software Development</td>
<td>Include security as a design requirement. Review all code and correct identified security flaws prior to deployment. Use of static code analysis tools recommended.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>16</td>
</tr>
</tbody>
</table>
## STANDARD

<table>
<thead>
<tr>
<th>STANDARD</th>
<th>WHAT TO DO</th>
<th>L</th>
<th>M</th>
<th>H</th>
<th>CSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>A9: Centralized Logging</td>
<td>Meet the Standard for Information Technology Logging requirements. Forward logs to University Central or ITSO authorized log server. Authorized log servers should provide a feed to the University Central log server.</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>8</td>
</tr>
<tr>
<td>A10: Security</td>
<td>Request a security review and implement recommendations prior to deployment/procurement.</td>
<td></td>
<td>✓</td>
<td></td>
<td>16</td>
</tr>
<tr>
<td>A11: Vulnerability Management</td>
<td>Perform a quarterly application scan. This is a requestable service catalog item. Remediate critical and high vulnerabilities within seven days of the scan.</td>
<td></td>
<td>✓</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>A12: Data Security Controls</td>
<td>Implement PCI DSS, FISMA, or export controls as applicable. Meet the Standard for High Risk Digital Data Protection requirements.</td>
<td></td>
<td>✓</td>
<td></td>
<td>3 6 13</td>
</tr>
</tbody>
</table>

## References

- Big Fix: [https://vt4help.service-now.com/sp?id=sc_cat_item&sys_id=13556b7b0ffed240d3254b9ce1050ed0](https://vt4help.service-now.com/sp?id=sc_cat_item&sys_id=13556b7b0ffed240d3254b9ce1050ed0)
- Network Backup Service: [https://vt4help.service-now.com/sp?id=sc_cat_item&sys_id=c13d337a0fd30a0005de498b1050efe](https://vt4help.service-now.com/sp?id=sc_cat_item&sys_id=c13d337a0fd30a0005de498b1050efe)
- Surplus Property: [https://security.vt.edu/resources/surplus.html](https://security.vt.edu/resources/surplus.html)
- Standard for IT Logging: [https://it.vt.edu/content/dam/it_vt_edu/policies/Standard_for_Information_Technology_Logging.pdf](https://it.vt.edu/content/dam/it_vt_edu/policies/Standard_for_Information_Technology_Logging.pdf)
- Standard for High Risk Digital Data Protection: [https://it.vt.edu/content/dam/it_vt_edu/policies/Standard-for-High-Risk-Digital-Data-Protection.pdf](https://it.vt.edu/content/dam/it_vt_edu/policies/Standard-for-High-Risk-Digital-Data-Protection.pdf)
- Vulnerability Scanning: [https://security.vt.edu/service/vulnerability_scanning.html](https://security.vt.edu/service/vulnerability_scanning.html)

## Maintenance of Standard

The IT Security Office is responsible for this IT Standard. Questions may be directed to security@vt.edu.

## Revisions

- Feb. 18 2020 – Boxes denoting which Critical Security Control applies to a particular element added. Whole disk encryption requirement removed for Low Risk Endpoints.
- June 16, 2020 - In the Endpoints section, this sentence: "Install antivirus (e.g. Windows Defender) and configure to automatically update and run scheduled scans" was changed to "install antivirus software if possible and configure to automatically update and run scheduled scans."
- July 21, 2021 – corrected some formatting errors.
October 27, 2021 – CIS numbers updated to V8. Encryption clause added to "Regulated Data Security Controls" sections, Standard for High Risk Digital Data Protection link added to References, version number, date updated.


V 3.5 Jan. 24, 2022 – Corrected formatting and updated links in References.

V 3.6 May, 2022 – Replaced “Centralized Logging” for Endpoints, Servers, Application wording with “Meet the Standard for Information Technology Logging requirements. Forward logs to University Central or ITSO authorized log server. Authorized log servers should provide a feed to the University Central log server.”

V 3.7 July 25, 2022 – Added line numbers to each item in the standard