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.

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

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.	✓	✓	✓	13
E7: Equipment Disposal	All university-owned equipment must go through Surplus Property for disposal.	✓	✓	✓	1
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.	✓	✓	✓	5, 6
E9: Configuration Management	Install BigFix or equivalent (Kaseya)			✓	4, 7
E10: Data Security Controls	Implement PCI DSS, FISMA, or export controls as applicable. Meet the Standard for High Risk Digital Data Protection requirements.			✓	3 6 13
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.			✓	8

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.

STANDARD	WHAT TO DO	L	M	H	CSC
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.	✓	✓	✓	7
S2: Inventory	Register your server with departmental inventory system. Send the ITSO a list of department's high risk servers.	✓	✓	✓	1, 7

STANDARD	WHAT TO DO	L	M	H	CSC
S3: Firewall	Enable host-based firewall in default deny mode and permit only the minimum necessary services.	✓	✓	✓	13
S4: Credentials, Access Control	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.	✓	✓	✓	5, 6
S5: Two-Factor Authentication	Require two-factor authentication for interactive user and administrator logins.	✓	✓	✓	5
S6: Equipment Disposal	All university-owned machines must go through Surplus Property for disposal.	✓	✓	✓	1
S7: Sysadmin Training	Attend at least one security training course annually.		✓	✓	14
S8: Malware Protection	Use Wazuh, OSSEC or equivalent security monitoring tool. Review alerts as they are received.		✓	✓	10
S9: Intrusion Detection	Use Wazuh, OSSEC or equivalent security monitoring tool. Review alerts as they are received.		✓	✓	13
S10: Physical Protection	Place system hardware in a data center or controlled access environment.		✓	✓	1
S11: 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.		✓	✓	8
S12: Security Review	Request a security review and implement recommendations prior to deployment.		✓	✓	6
S13: Vulnerability Management	Perform a quarterly scan. This is a requestable service catalog item. Resolve critical and high vulnerabilities within seven days of the scan.			✓	6
S14: Backups	Implement a backup & recovery process sufficient to restore the server to a trusted state. Maintain backups in a separate, offsite environment whenever possible.		✓	✓	11
S15: Data Security Controls	Implement PCI DSS, FISMA, or export controls as applicable. Meet the Standard for High Risk Digital Data Protection requirements.			✓	3 6 13

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.

STANDARD	WHAT TO DO	L	M	H	CSC
A1: 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 version of the application.	✓	✓	✓	16
A2: Inventory	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.	✓	✓	✓	2, 7
A3: Firewall	Permit the minimum necessary services through the application firewall.	✓	✓	✓	13,16
A4: Access Control	Review existing accounts and privileges at least annually. Enforce Virginia Tech Password Rules, Requirements and Tips.	✓	✓	✓	5,6
A5:Two Factor Authentication	Require two-factor authentication for interactive and administrator logins.	✓	✓	✓	4
A6: Backups	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.	✓	✓	✓	11
A7: Developer Training	Attend at least one security training course annually.		✓	✓	14 16
A8: Secure Software Development	Include security as a design requirement. Review all code and correct identified security flaws prior to deployment. Use of static code analysis tools recommended.		✓	✓	16

STANDARD	WHAT TO DO	L	M	H	CSC
A9: 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.			✓	8
A10: Security	Request a security review and implement recommendations prior to deployment/procurement.			✓	16
A11: Vulnerability Management	Perform a quarterly application scan. This is a requestable service catalog item. Remediate critical and high vulnerabilities within seven days of the scan.			✓	7
A12: Data Security Controls	Implement PCI DSS, FISMA, or export controls as applicable. Meet the Standard for High Risk Digital Data Protection requirements.			✓	3 6 13

References

Big Fix: 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=c13d337a0fd30a00005de498b1050efe

Surplus Property:
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

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

Vulnerability Scanning: 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.

Apr. 22, 2020 – added reference to “Wazuh” in the Malware Protection, Intrusion Detection section for Servers.

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.

Nov. 10, 2021 – Changed all references of “Regulated Data Security Controls” to “Data Security Controls. Replaced “Encrypt high risk data at rest and in transit” with “Meet the Standard for High Risk Digital Data Protection requirements.” in all of the renamed “Data Security Controls” sections. Replaced the existing “What to do” text for “Centralized Logging” (Servers, Applications) with “Meet the Standard for Information TechnologyLogging requirements”. Changed “Remediate” to “Resolve” in the What To Do section for Vulnerability Management (Servers). Changed “Whole Disk Encryption” phrase to “Encryption” in the Endpoint section.

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