Minimum Security Standard For University Maintained Technology

Revision: Version 2.2	Ratified: 6/23/2021	Status: APPROVED

Table of Contents

1. Objective

The objective of this standard is to clearly define the specific minimum technical and operational security practices needed to protect different types of University information resources based on the degree of risk that may be realized should these resources be compromised, stolen, degraded, or destroyed.

2. Scope

The standard applies to all Appalachian State University employees, students, affiliates, and all University IT services.

3. Requirements

3.1 IT Service Requirements

3.1.1 Inventory of University IT Services

ITS Support will lead cataloging of all IT services in an IT Service Catalog in coordination with ITS Project Management & Governance, University Data Stewards and Service owners. All Enterprise IT Services and University IT services that process or transmit Confidential Data must be included in an IT service inventory with designation of service owner, data classification of data transmitted/stored by the service, and System Impact level.

3.1.2 IT Service Owners

All University IT services must have an identified service owner. This is often a leadership position that has responsibility for ensuring that the appropriate resources and processes are established to operate the service. ITS Project Management and Governance will lead and manage processes related to this area.

3.1.3 IT Services and Associated System Impact Levels

In order to help determine required security levels, IT services will be assessed based on the types of University Data that they may process, store, or transmit as well as the overall potential impact that may be realized if the confidentiality, integrity, or availability of the service is lost or significantly degraded. ITS Project Management and Governance will lead processes related to this area.

University owned IT Systems that are directly used to operate a service inherit the overall impact level of that service. The University recognizes three IT service impact levels:

LOW IMPACT SERVICES	MEDIUM IMPACT SERVICES	HIGH IMPACT SERVICES
University IT Services and Associated Systems are classified as Low Impact if:	University IT Services and Associated Systems are classified as Medium Impact if:	University IT Services and Associated Systems are classified as High Impact if they:
1. The data store is intended for public disclosure (Public Data). **-or-** 2. The loss of confidentiality,	1. They process, transmit, or store **Internal** or **Sensitive** data but not Confidential Data. **-or-**	1. Process, transmit, or store **Confidential** data. **-or-** 2. The loss of confidentiality, integrity, or availability of the

integrity, or availability of the service and associated systems would have a minimal adverse impact on our mission, safety, finances, or reputation.	2. The loss of confidentiality, integrity, or availability of the service and associated systems would have a moderate impact on our mission, safety, finances, or reputation.	service and associated systems would reasonably result in significant financial losses, unacceptable risks, or impairment to the efficient conduct of the University's mission.

3.2 Minimum Security Baseline Requirements

The information below defines the minimum degree of security required for University managed end user devices, Infrastructure, and Applications. Per the University Secure Storage and Sharing Guidelines, personally owned devices including mobile devices such as smartphones and tablets should not store, process, or transmit Confidential or Sensitive University data.

3.2.1 Managed End User Devices: Minimum Requirements

Control Area	What To Do	Low Impact	Medium Impact	High Impact
Patching	Apply all applicable OS and Application Security Updates within no more than 14 days of publication, unless a shorter timeline is determined to be necessary by the CIO/CISO or apply applicable compensating controls/workarounds. Apply all other security patches within 90 days. All Institutional end user devices must use a supported OS version. Patch Deferment - System Administrators may defer patches beyond 14 days if they determine them to be unreliable at time of release or present other appreciable operational risks. Deferred patches must be documented and periodically reviewed and should not exceed 30 days without joint review with the ITS Office of Information Security.	✓	✓	✓
Firewall	Enable host-based firewall in default deny for inbound connections and permit only minimum necessary services.	✓	✓	✓

Whole Disk Encryption* (windows, mac, linux coming)	Where technically feasible, endpoints must be encrypted by ITS. *Available Solutions: Bitlocker, Filevault*	✓	✓	✓
Malware Protection	Endpoints will utilize an ITS approved malware protection solution. *Approved Solutions: Cisco AMP*	✓	✓	✓
Intrusion Prevention & Detection	Endpoints will utilize an ITS approved intrusion detection solution. *Approved Solutions: Cisco AMP*	✓	✓	✓
Centralized Logging	A centrally maintained data shipping agent must be deployed on endpoints and forward selected log feeds to ITS log repository. *Available Solutions: Elastic Beats*	✓	✓	✓
Configuration Management	University owned end user devices must be centrally managed by ITS using a central device management system. An ITS-OIS provided configuration and compliance management agent must be installed to periodically validate configuration states. *Available Management Solutions: JAMF Suite (macOS/iOS) or SCCM/GP/Azure/InTune (Windows).*	✓	✓	✓
Time Synchronization	Endpoint must have system clock synchronized to an authoritative time server.		✓	✓
Inventory	An inventory must be kept of endpoints that periodically store confidential data. *Available Solutions: Insight Asset Management*			✓
Confidential Data Discovery	Data Loss Prevention software must be installed and automated scans performed at least once a month. *Available Solutions: Spirion*			✓

Regulated Data Security Controls	Implement PCI-DSS or HIPAA controls if applicable.			✓

3.2.2 Infrastructure Baseline Requirements

Control Area	What To Do	Low Impact	Medium Impact	High Impact
Patching	Based on National Vulnerability Database (NVD) CVSS 2.0 ratings, apply high severity security patches within 7 days of release or when ITS becomes aware of the security notice, unless a shorter timeline is determined to be necessary by the CIO/CISO or apply applicable compensating controls or workarounds. Apply all other security patches within 90 days. All Infrastructure must use a supported OS or firmware version. Guaranteed Quarterly Weekend Patch windows will be created and used for deploying patches on systems that require longer maintenance windows or outages. **Deferring Patching** - System Administrators may approve any deferment of low and medium severity patches beyond 90 days based on review of operational risks involving quality of patches, operational impact of patching, cycles of business operations, recommended patch level of vendor, or availability of mitigation controls. - High severity patches may only be deferred beyond 7 days with approval by IT Leadership. - Deferred patches must be documented in a central repository and periodically reviewed.	✓	✓	✓

Firewall	Enable host or device based firewalls in default deny mode for inbound connections and permit minimum necessary services. Systems that do not have the ability to run a local firewall, should make use of network based firewalls as compensating control.	✓	✓	✓
Intrusion Detection & Prevention	Infrastructure will utilize an ITS approved intrusion detection and prevention solution. Appliance based systems that cannot run IDP software are excluded from this requirement. *Approved Solutions: Cisco AMP*	✓	✓	✓
Centralized Logging	A centrally maintained data shipping agent must be deployed on all systems (where possible). Selected Logs from systems will be required to be sent to the ITS ELK Logging system. These Logs will be made available to OIS, System Administrators, and other persons or entities as determined by ITS Leadership. *Available Solutions: Elastic Beats or Device Provided Logging*	✓	✓	✓
Vulnerability Scanning	At least monthly, OIS and ITIS will coordinate the scanning of Infrastructure for vulnerabilities using an ITS-OIS approved scanning solution and method. Results of the scans will be shared with OIS, System Administrators, and ITS Leadership. *Approved Solutions: Rapid 7 (authenticated scans, agent based scans, or external scanning for systems that do not support authenticated or agent based scans.)*		✓	✓
Time Synchronization	Infrastructure must have their system clocks synchronized to an authoritative Time server.		✓	✓
Physical Protection	On premise Infrastructure must be placed in an ITS maintained Data Center. All Networking equipment must be in a locked environment with limited access control. Physical management console ports should be password protected.		✓	✓

Two Step Authentication*	Where technically feasible, Infrastructure must have Duo two-factor authentication for all interactive user and administrator logins.			✓
Inventory	An inventory must be kept of Infrastructure that store, process, or transmit confidential data.			✓
Sysadmin Training	System administrators will receive training on relevant security threats and controls.			✓
Security Review	Request a security review from ITS and OIS and discuss recommendations prior to deployment. During initial discussions a timeline will be established for completion.			✓
Regulated Data Security Controls	Implement PCI-DSS or HIPAA controls if applicable. De-scoping control obligations must be a priority.			✓
SNMP	If SNMP is used, community strings must be updated and not utilize defaults (“public”, “private”). SNMPv3 must be used if available.			✓
Configuration Management & Auditing	Change logs must be maintained for overall configuration and firmware updates. Where applicable, configuration should be reviewed by automated or manual means to review for any unauthorized or unapproved changes to configuration.			✓

3.2.3 Application Baseline Requirements

Control Area	What To Do	Low Impact	Medium Impact	High Impact
Patching	Based on National Vulnerability Database (NVD) ratings, apply high severity security patches within 7 days of publish, medium severity within 14 days, and low severity within 28 days, unless a shorter timeline is determined to be necessary by the CIO/CISO or apply applicable compensating controls/workarounds. Apply all other security patches within 90 days.	✓	✓	✓

	All institutional applications must run on a supported OS version.			
Credentials and Access Control	Review existing accounts and privileges at least quarterly. Enforce password complexity. Logins with AppState credentials recommended to use Shibboleth. Or AD (see Identity and Access Management).	✓	✓	✓
Inventory	An inventory must be kept of applications that store, process, or transmit confidential data.			✓
Secure Software Development	Include security as a design requirement. Review all code and correct identified security flaws before deployment. Use of dynamic and static code analysis tools recommended.			✓
Two Step Authentication	Where technically feasible, Implement two-factor authentication for all interactive user and administrator logins.	✓	✓	✓
Centralized Logging	A centrally maintained data shipping agent must be deployed on servers and forward selected application log feeds to ITS SIEM.		✓	✓
Vulnerability Management	Web applications vulnerability scans should be performed and results reviewed at least once per month			✓
Security Review	Request a security review from ITS and OIS and discuss recommendations prior to deployment. During initial discussions a timeline will be established for completion.			✓
Regulated Data Security Controls	Implement PCI-DSS or HIPAA controls if applicable.			✓

3.3 Enforcement, Exemptions, and Advisement

3.3.1 Authority and Enforceability - This standard is established under the authority of the University Chief Information Officer (Information Security Policy 4.3.3). In the event of violation of this standard, the University Chief Information Officer or Chief Information Security Officer may

require that non-compliant University IT services be disconnected or temporarily suspended until the minimum security controls (see section 3.3) are established and/or verified.

3.3.2 Exemptions - Exemptions to this standard must undergo a formal risk evaluation and receive documented approval by the University Chief Information Officer or Chief Information Security Officer.

3.3.3 Review and Advisement - Collaborative advisement concerning these standards are provided by the University IT Security Liaisons Group and Campus Information Security Advisory Committee.

4. Definitions

4.1 IT Services: IT services refers to the application of business and technical expertise to enable the creation, management and optimization of or access to information and business processes and includes business process services, application services and infrastructure services.

4.2 End User Device: any laptop, desktop, mobile device, or computing instrument used to support or conduct official University business. Also referred to as an endpoint.

4.3 Managed end user device: End user devices that are enrolled in an Appalachian State University device management system

4.5 Server: A server is a host or device that provides a network accessible service.

4.6 Institutional Data: All data, regardless of physical form or characteristic, made or received in connection with the transaction of University business that is in the possession or control of the University.

4.7 Application: An application is software running on a server that is remotely accessible.

5. References

5.1 University Information Security Policy

5.2 University Data Management Standard

5.3 University Statement of Confidentiality

5.4 University Identity Theft Prevention Plan

5.5 University Payment Card Services Policy