DEVICE CONFIGURATION STANDARDS

The capitalized terms used herein are defined in the Device Configuration Management policy.

Northern Arizona University owns, controls, or acts as custodian for a broad array of information, including Sensitive Information protected by law or regulation. Maintaining the integrity of this data and the information systems where it is stored is an important obligation. To support this crucial task, the University has established the device configuration standards outlined in this document. These standards apply to three separate categories of devices, which are: a) University servers; b) University desktops, laptops, tablets, and all other mobile computing devices (collectively referred to as "Endpoints"")' and c) all types of non-University computing devices (collectively referred to as "Personal Devices").

These device configuration standards are an extension of the University's *Device Configuration Management* policy. They are revised or updated as appropriate by the Chief Information Officer ("CIO"), or their designee, and are based on the four data classifications described in the University's Data Classification and Handling policy, which are:

- **Level 1 Public Data – Very Low Risk**
- **Level 2 Internal Data – Low Risk**
- **Level 3 Sensitive Data – High Risk**
- **Level 4 Highly Sensitive Data – Very High Risk**

In accordance with the *Data Classification and Handling* policy, all University Community Members and units, wherever located, are required to classify all University data within their care and to implement the appropriate device configuration standards as outlined below. Contact the appropriate Data Steward, the Chief Institutional Data Officer, or Information Technology Services with questions or to request assistance with appropriate classification of specific data types and to implement the most appropriate methods of protection.

These device configuration standards represent the minimum baseline approach for protecting and securely handling Sensitive Information on the University's servers, Endpoints, and non-University Personal Devices that connect with the University's information systems or networks, and/or the network equipment itself for the purpose of conducting official University business. In special circumstances, such as when a data type is subject to special legal or regulatory control (*e.g.*, health, financial, or research information), additional controls may be necessary or advisable. Contact the CIO, or their designee, or Information Security Services for assistance with such situations.

To apply the appropriate device configuration standard:

1. Jump to the appropriate device category below depending on whether you are configuring a server, an Endpoint, or a Personal Device. For servers, also review the server security standards. For network equipment, look for configuration standards within the server categories; as all data classifications traverse the network and through these devices, they should follow similar standards especially for Level 4 Highly Sensitive Data.

2. Identify the appropriate data classification level that applies from the four categories delineated above. (The *Data Classification and Handling* policy provides additional guidance on proper classification of data.) If multiple data levels are present, select the highest applicable classification.

3. Use the matrices that follow to identify each device configuration standard.

a. "N" or "No Restrictions" means the data can be publicly disclosed without limitations;
b. "E" or "Encouraged" means the data should remain confidential when possible but that such confidentiality is not required;
c. "R" or "Required" means the data must remain confidential in accordance with all applicable laws, regulations, policies, and/or contractual obligations. Exceptions may be granted on a case-by-case basis with the approval of the CIO or their designee; and
d. "M" or "Mandatory" means that maintaining the data's confidentiality in strict adherence to all privacy and security protections as set forth in all applicable laws, regulations, policies, and/or contractual obligations is mandatory. Exceptions may NOT be granted by NAU alone but may be approved in conjunction with other external parities on a case-by-case basis.
e.

In the "Description" column, links are provided to any applicable Information Security Standard or to other relevant or helpful information. View the Information Security policy for more information about the University's Information Security Standards.

SECTION I. – SERVER CONFIGURATION STANDARDS

Device Configuration Standard	Description	Level 1	Level 2	Level 3	Level 4
Physical Protection (applies to networking devices)	Server protected by physical access controls	E	E	M	M
	Server hosted in an approved ITS facility with access monitored, logged, and limited to authorized individuals only	E	E	M	M
Patching (applies to networking devices)	Keep all software up to date on a regular and consistent schedule as identified in the URL above, especially high or critical severity patches	M	M	M	M
	Test and validate security patches before deployment to production environments when available	~~E~~M	M	M	M
Malware Protection	Install Microsoft Defender on eligible servers	M	M	M	M
	Update Microsoft Defender daily	M	M	M	M
Media Disposal (applies to networking devices)	Deleting or reformatting media is not sufficient for securing data, data must be disposed of~~dis~~ ~~F~~ by following ~~industry standards~~ the guidelines provided in the current version of NIST-SP-800-88 Guidelines for Media Sanitization~~for secure wiping – deleting or reformatting media is not sufficient –~~ prior to transfer or removal	E	E	M	M
	Research data must be approved by the Office of the Vice President for Research before it may be transferred	E	E	M	M

Device Configuration Standard	Description	Level 1	Level 2	Level 3	Level 4
Encryption (applies to networking devices)	Stored data should be encrypted with full-disk encryption	E	RME	M	M
	Transmission of data should be encrypted	E	ERM	M	M
	Where TLS/SSL certificates are used, only secure protocols and cipher suites must be used and the certificate must be signed by a well trusted authority such as Sectigo/Incommon or Let's Encrypt or a centrally managed locally trusted CA and invalid certs should never be used	E	REM	M	M
Backup and Recovery	Backups to a CIO's, or their designee's, -approved solution is mandatory	M	M	M	M
	Backups should be encrypted in transit and at rest	E	ERM	RME	M
Access Controls (applies to networking devices)	Access must be provisioned based on the level of need with least-privilege as the guiding principle	E	M	M	M
	Approval from a manager or data steward must be obtained and documented	E	M	M	M
	Access is reviewed regularly (annually at minimum) and must be terminated when no longer needed	E	M	M	M
	Access to is a unique account per individual and all University Community Members must comply with the Appropriate Use of Information Technology Resources policy	M	M	M	M
Remote Access (applies to networking devices)	Remote access is restricted to a list of authorized hosts, a secure VPN group, or bastion host and must be encrypted. ~~Remote access should is be restricted to a local network, a secure VPN group, or bastion host and must be encrypted~~	M	M	M	M
	Remote access to servers ~~should~~ requires multi-factor authentication	E	E	M	M
	Remote access may only be completed through approved methods	R	R	R	R
	Services in operating systems that allow for remote access must not be exposed to external networks	R	R	R	R

Device Configuration Standard	Description	Level 1	Level 2	Level 3	Level 4
Activity Logging (applies to networking devices)	Activity logging and monitoring should be enabled and follow the standards outlined in the Audit, Logging, and Monitoring Standards	E	EM	M	M
Firewall (applies to networking devices)	Network firewalls must be configured to block ports following a default "deny-all" rule for inbound traffic, except those necessary for running the services required by the server role – OR - Host based firewalls must be enabled and configured to block ports following a default "deny-all" rule for inbound traffic, except those necessary for running the services required by the server role	MER	MR	MR	MR
Change Management (applies to networking devices)	Change management controls will be implemented, followed, and documented for the University's IT Resource production environment	M	M	M	M
Configuration Management	Windows servers must be domain joined All servers must participate in CMDB All servers must participate in appropriate configuration management systems, e.g. SCCM, JAMF, Ansible	ME EM E	EM ME E	ME ME E	ME ME E
Vulnerability Management (applies to networking devices)	Vulnerability Management and Scanning All servers attached to University's network will be scanned on a regular and consistent schedule as identified in the *Vulnerability Management and Scanning* Information Security Standard and must follow remediation plans as outlined	M	M	M	M

SECTION II. – SERVER SECURITY STANDARDS

The server security standards outlined below represent the minimum allowable baseline for the protection and secure handling of Sensitive Information on all servers owned by the University or operated on the University's behalf, wherever located. Additional controls, as determined by the CIO, or their designee, acting through the Director of Information Security, may be necessary or advisable in special circumstances, such as when a data type is governed by applicable law or regulations (*e.g.*, health, financial, or research information). Contact the

CIO, or their designee, or Information Security Services to request assistance or for more information regarding such situations or these server security standards.

A. Ownership and Responsibility

All servers shall be managed by an individual or team of qualified System Administrators who shall be responsible for the system's proper configuration in accordance with the standards outlined in this or other relevant or applicable policy documents. The responsible System Administrators shall establish and maintain appropriate server configuration baselines and protocols that reflect and respond to the server's purpose and business function. Information Security Services shall review these materials periodically as necessary or appropriate. System Administrators are responsible for establishing and administering set processes for maintaining and updating their server configuration baselines and protocols, and for documenting their server configurations and any approved exceptions or alternative security controls. Specifically, System Administrators are responsible for documenting the following information for each server they administer:

- Server contact(s) and physical location
- Network address and hostname(s)
- Operating system version
- Software packages – name, vendor, version
- Description of server primary functions, roles, services
- Data levels stored, transmitted, or processed

B. General Configuration Requirements

In addition to the Information Security policy and its ancillary set of Information Security Standards, all System Administrators are responsible for assuring the following general configuration requirements:

- Services and applications not in use must be disabled where practical
- Default passwords must be changed
- Use private IP addresses unless public accessibility is required
- Use a WAF such as modsec or Netscaler WAF where possible to protect web services
- Standard security principles of least access required to perform a function must always be used
- Use of 'root' or 'administrator' must never be used when a non-privileged account can be used
- Re-use of a local privileged account and password across multiple systems should not occur (instead create server-specific local account/password unique to each system)
- Use the most restrictive trust relationship possible as simple trust relationships between IT Resources are a security risk and should be kept to a minimum or avoided

C. Baseline Server Configuration Guidelines

Information Technology Services maintains the following Windows and Linux server configuration guidelines and best practices. System Administrators shall use this guidance to help secure servers on the University's network and, therefore, to help protect the data stored, processed, or transmitted using these devices. These guidance documents are intended to provide baseline descriptions of a System Administrator's server administration responsibilities as outlined above.

Windows Server Configuration Guidelines

Linux Server Configuration Guidelines

SECTION III. – ENDPOINT CONFIGURATION STANDARDS

Device Configuration Standard	Description	Level 1	Level 2	Level 3	Level 4
Physical Protection	Endpoints will be kept in a physically secure location when not in an individual's direct possession. Laptops and mobile devices involved with highly sensitive data including research must be locked and stored when not in use.	E	E	M	M
	Endpoints which are stolen, lost or misplaced must have a report made to the Northern Arizona University Police Department or other law enforcement agency of jurisdiction.	M	M	M	M
	Remote wipe and device recovery software on laptops and mobile devices **may be necessary** for certain data agreements	E	E	E / M	E / M
Patching	Keep all software up to date on a regular and consistent schedule as identified in the URL above, especially High/Critical Severity patches	M	M	M	M
	Software and apps should be installed and updated from trusted sources only and configured to limit the information made available to the app (example: disable or turn off the location-based services wherever it is not needed).	E	E	M	M
Malware Protection	Install Microsoft Defender on all eligible endpoints	M	M	M	M
	Update Microsoft Defender daily	M	M	M	M
Media Disposal	Follow industry standards for secure wiping—deleting or reformatting media is not sufficient—prior to transfer or removal	E	M	M	M
	Research data must be approved by the Office of the Vice President for Research before it may be transferred	E	E	M	M
	Remote wipe and device recovery software on laptops and mobile devices may be necessary for certain data agreements	E	E	E / M	E / M
Encryption	**Institutional data should not be stored on Endpoints**, but if necessary, the data should be encrypted with full disk encryption via BitLocker for Windows, FileVault for Macintosh)	E	RM~~E~~	M	M
	Transmission, or sending, of data should be encrypted and is required for highly sensitive data types	E	RM~~E~~	M	M

Device Configuration Standard	Description	Level 1	Level 2	Level 3	Level 4
Backup and Recovery	**Institutional data should not be stored on Endpoints**				
	Backups to a CIO's, or their designee's,-approved solution is required	E	M	M	M
	Backups must be encrypted	E	RE	M	M
Access Controls	Where possible, Endpoints will be password protected when unattended and configured to automatically lock the screen after 15 minutes or less of inactivity.	E	M	M	M
	Access should be via unique account per individual and all University Community Members must comply with the Appropriate Use of Information Technology Resources policy	E	M	M	M
	~~Where possible, limit the use of Administrator accounts for system administration services only~~Use of Administrative accounts are prohibited unless an exception has been approved	E RE	E ER	M M	M M
	Mobile devices must be password or pin code protected				
	Endpoints that support a BIOS password must have it enabled.	R	R	R	R
Remote Access	Remote Access should be restricted to a local network, a secure VPN group, bastion host	E	M	M	M
	Remote access to servers should require multi-factor authentication	E	E	M	M
	Remote access may only be completed through approved methods: Microsoft Remote Access, BeyondTrust, ~~and~~\ Secure Shell (SSH)~~.~~ Exceptions to this policy must have an explicit business justification and be approved by the CIO, or their designee.	R	R	R	R
Firewall	Host based firewalls must be enabled and configured to deny inbound connections unless needed by IT configuration management or update systems	E	M	M	M
Configuration Management	Windows and Macintosh Endpoints must be domain joined	E	E	M	M
	All Endpoints must participate in appropriate configuration management systems, e.g. SCCM, JAMF, Ansible.	E	E	M	M

Device Configuration Standard	Description	Level 1	Level 2	Level 3	Level 4
	Endpoints that support secure boot must have it enabled.	R	R	R	R

SECTION IV. – ENDPOINT SECURITY STANDARDS

Adhering to security best practices and the principle of Least Privilege NAU's default configuration on all endpoints will not include Administrative ~~a~~Accounts or ~~a~~Access. University Community Members who require the ability to install approved software on a NAU endpoint may call the ServiceDesk ~~(~~ ~~)~~ at (928)523-3335 to request Administrative access for a limited time. University Community Members who require regular Administrative access to complete their assigned job responsibilities may request an exception. All exceptions must include a clear and active business need, supported by thorough justification. This justification be approved by the University Community Members's Supervisor and ISS. These exceptions must be renewed on a yearly basis.

SECTION V. -- PERSONAL DEVICES

The increasing use of mobile computing devices, including but not limited to, personally owned smartphones and tablet computers, has resulted in an increased ability for University Community Members to work from anywhere. These mobile devices provide convenience and productivity gains, but they also increase the risk of data loss and theft if the device is lost, stolen, or compromised. Additional risks include possible violation of University contracts or state or federal laws and regulations. Accordingly, individuals using Personal Devices to access the University's Sensitive Information are required to know and comply with the following:

1. Approved Devices and Support

Any computing device may be connected to the University guest, secure, or eduroam wireless networks provided the device use does not disrupt University IT Resources or violate the *Appropriate Use of Information Technology Resources Policy*. The secure and eduroam networks require authentication for use and users are required to follow all policies and standards for acceptable use. When within its coverage area, University Community Members must use the University's secure wireless network when handling University information or data on a wireless device.

1.1. The University will maintain the availability of its network.

1.2. The University will maintain the availability of its network authentication systems.

1.3. The University will provide limited support to University Community Members, including:
- 1.3.1. Documentation and guidance for configuring email on Personal Devices
- 1.3.2. Documentation and guidance for configuring and use of VPN on Personal Devices
- 1.3.3. Documentation and guidance for connecting to network drives
- 1.3.4. Wireless compatibility for officially supported device types
- 1.3.5.Assessment and removal of viruses, malware, spyware

1.4. The University will NOT provide the following support for faculty, staff, or affiliate Personal Devices:
- 1.4.1. Performance issues
- 1.4.2. Hardware problems
- 1.4.3. Applications
- 1.4.4. Operating system upgrades or patches
- 1.4.5. Backing up data or migrating data to other devices

1.5. The University will provide the following support for student Personal Devices:

1.5.1. Support for University provided software. Including, but not limited to, University Gmail and Google G Suite for Education, Office 365, and Blackboard Learn

1.5.2. Virus and malware removal

1.5.3. Connecting to and troubleshooting issues with University network connections

1.5.4. Performance issues and system crashes

1.5.5. Hardware problem diagnosis, limited repairs, replacements, and upgrades. Purchase of equipment/parts is the responsibility of the student

1.5.6. Operating system re-installations, upgrades, and patches

1.5.7. Limited data recovery and backup

2. User Responsibilities

Individuals using Personal Devices to access Sensitive Information must abide by all applicable University policies, including the *Appropriate Use of Information Technology Resources* policy, *Information Security* policy and its related standards, the *Device Configuration Management* policy, and the *Data Classification and Handling* policy. When within its coverage area, University Community Members must use the University's secure wireless network when handling University information or data on a wireless device.

2.1. Ensure any Personal Devices accessing or storing University data meets or exceeds the standards set in Section III. – Endpoint Configuration Standards

~~2.1.~~**2.2.** Do not download or store Level 3 – Sensitive Data or Level 4 – Highly Sensitive Data on Personal Devices.

~~2.2.~~**2.3.** Destroy or remove and return all data belonging to the University upon departure from the University or when the Personal Device is sold/transferred.

~~2.3.~~**2.4.** The theft or loss of any Personal Devices containing University data must be reported to the Northern Arizona University Police Department or other law enforcement agency of jurisdiction.

~~2.4.~~**2.5.** Follow the standards and guidelines outlined in the *Device Configuration Management* policy and standards to implement safeguards to protect University data.

~~2.5.~~**2.6.** Users are responsible for anyone who uses the device, including, but not limited to, significant others, spouse, roommates, children, etc.

3. Conditions, Risks, Liabilities, Disclaimers

University Community Members who use a Personal Device in furtherance of their job responsibilities or to conduct University business may do so only after accepting and acknowledging the conditions, risks, liabilities, and disclaimers outlined below. University Community Members who are unwilling to do so are encouraged in the alternative to use University-provided computing devices to fulfil their work obligations.

3.1. The University at no time accepts liability for the maintenance, backup, or loss of data on a Personal Device. It is the full responsibility of the device owner to backup Personal Device software and data.

3.2. The University at no time will be liable for the loss, theft, or damage of a Personal Device. This includes, and is not limited to, when the device is being used for University business or during University travel.

3.3. The University reserves the right to implement technology such as Mobile Device Management ("MDM") and/or Network Access Control ("NAC") to enable the management of and the removal of University Information or data from Personal Devices that access its IT networks.

3.4. As permitted by law, the University may request that a University Community Member permit inspection of or provide appropriate access to University Information or data stored on their Personal Device when

doing so is necessary for the University to effectively administer its IT Resources, maintain the integrity of Sensitive Information, enforce its policies, uphold its contractual obligations, or fulfill its legal duties.

4. Security and Monitoring

The University reserves the right to implement technology such as MDM and/or NAC to enable the management, monitoring, and restriction of devices that access the University's IT networks.

4.1. The University may perform vulnerability scanning, network scanning, and security scanning on Personal Devices that access the University's IT networks.

4.2. As outlined in the University's *Information Security* policy, when necessary to protect the integrity or security of its IT Resources or information systems and the University Information they contain, the University may suspend access to its networks or devices (including Personal Devices) and may examine any user account. At the discretion of the CIO, ~~-~~or their designee, enforcement of this and related IT policies may include the removal of devices or systems from the University's information networks until compliance with applicable requirements is achieved. Violations by a University Community Member of the duty and responsibility to protect the University's data, IT Resources, and information systems in accordance with this and other applicable policies, standards, or requirements may also result in denial of access to University Information and/or University IT Resources or the temporary or permanent revocation of access privileges. Individuals who violate this policy are subject to disciplinary action under applicable Arizona Board of Regents and University conduct policies up to and including expulsion or termination and possible civil liability or criminal prosecution. In cases where full compliance with the requirements of this policy may not be immediately achievable, the unit's leadership must consult with Information Security Services to develop a plan for achieving compliance as soon as possible.

5. Sensitive Data Breach Response Protocols

5.1. Immediate reporting to Information Security Services of any suspected or actual release or breach of sensitive data, systems, or devices is mandatory. **Dial 928-523-3335 to make a report.**

5.2. Upon receiving a report of suspected or actual release or breach of sensitive data, systems, or devices Information Security Services will in collaboration with affected University stakeholders notify all affected or responsible parties as appropriate.

5.3. The CIO, or their designee, will assemble an incident response team to investigate, preserve evidence, mitigate, and report on the event.

5.4. In incidences where health or safety may be a concern, the reporting party or Information Security Services will immediately notify the Northern Arizona University Police Department and any external authorities as may be appropriate.

SECTION V. – EXCEPTIONS

If minimum baseline standards cannot be met the resource owner may request an exception by opening a ServiceNow Ticket with the ISS Team. This ticket should include:

- Why the standard cannot be met
- What risk mitigations have you put in place
- What other options have you explored

Exceptions may be granted after a consultation on a case-by-case basis~~.~~ Exceptions must be renewed on a yearly basis.

~~5.4.~~