DEVICE CONFIGURATION MANAGEMENT

Effective Date: July 24, 2019

y applicable Information Security Standard or to other relevant or helpful information. View the Information Security policy for more information about 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)	Secure Data Center Physical Security Server protected by physical access controls Server hosted in an approved ITS facility with access monitored, logged, and limited to authorized individuals only				

Device Configuration Standard	

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
U 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 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

Device Configuration Standard	Description	Level 1	Level 2	Level 3	Level 4
	disable or turn off the location-based services wherever it is not needed).				
Malware Protection	Install anti-virus software on all eligible endpoints Update anti-virus software daily				

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 IT networks.

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

4.2. *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, enforcement of this and related IT policies may

with applicable requirements is achieved. Violations by a University Community Member of the duty 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

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 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.