Responsible Executive: Chief Information Officer
Responsible Office: Information Technology Services
Effective Date: July 24, 2019
Last Revised: August 19, 2022

DEVICE CONFIGURATION MANAGEMENT

POLICY SUMMARY

Northern Arizona University owns or controls, and acts as custodian for, a broad array of information, including Sensitive Information protected by law. Maintaining the integrity of this data and the information systems where it is stored is an important obligation. This policy establishes baseline controls and standards for the management and maintenance of the Universityõs Information Technology (ñITò) Resources in support of this crucial task. All units and University Community Members are responsible for classifying all data within their care and implementing appropriate device configuration standards to protect the data.

REASON FOR THIS POLICY

Clear configuration standards and controls for servers, Endpoints, and mobile devices (especially those that transmit or store Sensitive Information, provide network connections, or function as part of authentication, authorization, or access control systems) help protect against vulnerabilities, minimize the risk of unauthorized access, and maintain system, data, and device integrity.

ENTITIES AFFECTED BY THIS POLICY

All units that handle or interact with University data and information systems
Information Security Committee
Information Technology Services

WHO SHOULD KNOW THIS POLICY

All University Community Members who interact with University data and information systems
Chief Information Officer (ñCIOò)
Director, Information Security Services
System Administrators
Technicians

DEFINITIONS

Endpoint: any network-connected device, including, but not limited to, University desktops, laptops, tablets, and mobile devices.

Personal Device: any computer, server, communication or mobile device, data storage, transmission or control device not owned or operated by the University, but that could be used to conduct University business to access Sensitive Information. This includes devices acquired for personal use but used to process, store, or transmit University data.

Sensitive Information: all information that should remain private or confidential as designated by the University or as required by law, including, but not limited to, educational and student conduct records, social security numbers, credit card or banking information, regulated research data, and health care provider records. Sensitive Information includes, but is not limited to, Level 3 ï Sensitive Data and Level 4 ï Highly Sensitive Data as defined in the Universityõs *Data Handling and Classification* policy.

System Administrators: University employees responsible for configuring, administering and maintaining University IT Resources for use by Authorized Users for authorized purposes.

Technicians: University employees who configure, maintain, or repair University IT Resources.

1. Physical protection
2. Patching
3. Malware protection
4. Media disposal
5. Encryption
6. Backup and recovery
7. Access controls
8. Remote access
9. Firewalls

E. Compliance and Enforcement

Information Security

Sources

Arizona Board of Regents Policy 9-201

Arizona Board of Regents Policy 9-202