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

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 University's Information Technology ("IT") 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 ("CIO")
- 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 – Sensitive Data and Level 4 – Highly Sensitive Data as defined in the University's *Data Handling and Classification* policy.

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

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

University Community Member: all University faculty, staff, student employees, students, alumni, affiliates, contractors, consultants, agents, and volunteers wherever located.

University Information Technology ("IT") Resource: any computer, server, communication or mobile device, or electronic data, data storage, transmission or control device that is owned and/or operated by the University. These resources are referred to herein as "University IT Resources."

Policy

A. Personal Devices

All Personal Devices used to access Sensitive Information must adhere to section IV of the Device Configuration Standards that accompany this policy. This document outlines the appropriate uses, device settings, procedures, responsibilities, and the conditions, risks, and liabilities associated with using Personal Devices to fulfill professional obligations such as accessing or working with Sensitive Information. Additionally, all such users are responsible for knowing and complying with the *Data Classification and Handling* policy.

B. University IT Resources

This policy applies to and governs all University IT Resources wherever located. Each University unit is required to classify all data within its care or control and to implement the appropriate device configuration standards for each University computer or other IT Resource under its management or jurisdiction. Information Technology Services is available to assist in this regard. All units, however, are individually responsible for ensuring implementation of the correct data classification and device configuration settings as outlined in the University's *Data Classification and Handling* policy and *Device Configuration Standards* document.

C. University IT Resource Configuration Baselines

System Administrators and Technicians configuring, installing, or deploying new University IT Resources must maintain secure configuration baselines for servers, Endpoints, and other digital services that host data. Baseline configurations shall conform to industry best practices and may be created from pre-built configuration templates. System Administrators and Technicians may develop their own configuration baselines and may modify a pre-built template to create a new baseline. In all instances, the configuration baseline must be documented, reviewed, and updated at least annually or upon significant changes to information system functions, roles, or architecture. Documentation must identify the template in use or the configuration settings where templates are not employed. One previous version, at a minimum, of a configuration baseline must be retained to support rollback and recovery. The current and previous versions of configuration baselines must be stored in a secure location. Validation and confirmation of configuration settings is strongly encouraged and may be done via automated tools such as the NIST Security Content Automation Protocol ("SCAP") validation program or as part of the University's Vulnerability Management program.

D. University IT Resource Configuration Standards

The CIO, or their designee, shall establish, update, revise, and republish as necessary and appropriate comprehensive *Device Configuration Standards* designed to enhance the protection of and to reflect the data type classifications established and outlined in the University's *Data Classification and Handling* policy. Of particular concern are devices that transmit or store Sensitive Information, provide network connections, or function as part of authentication, authorization, or access control systems. The configuration standards must be documented, reviewed, and updated at least annually. Accordingly, these *Device Configuration Standards* will apply to all data processing or computing devices capable of connecting to or interacting with the University's IT networks and shall reflect and promote data handling best practices and compliance with all applicable laws, regulations, policies, and contractual or licensing requirements. At minimum, these standards shall cover or address the following:

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
~~9.~~10. Configuration Management

E. Compliance and Enforcement

As outlined in the University's *Information Security* policy, when necessary to protect the integrity or security of its University IT Resources or information systems and the University Information they contain, the University may suspend access to its networks or 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, University 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.

Responsibilities

Chief Information Officer: in collaboration with the Director of Information Security Services, update as necessary and appropriate and enforces the University's *Device Configuration Standards*.

System Administrators and Technicians: maintain configuration baselines; deploy configuration settings or images to information systems; maintain the privacy and confidentiality of personal or University information that is accessed, viewed, or obtained in the normal course of their work report suspected or actual violations of the University IT-related policies to the appropriate University authority.

University Community Members: ensure the effective implementation and enforcement of this policy within their respective areas of responsibility or jurisdiction.

Procedures

There are no procedures associated with this policy.

Related Information

Forms or Tools

Device Configuration Standards

Cross-References

Appropriate Use of Information Technology Resources

Data Classification and Handling

Information Security

Sources

Arizona Board of Regents Policy 9-201

Arizona Board of Regents Policy 9-202

APPENDIX

None.