University of Alaska Office of Information Technology System Security Guidelines

The university computing environment is made up of a variety of operating systems, devices and applications. Inasmuch as the following classes of controls apply to each of those things and technical controls exist the guidance below should be a default state and exceptions documented.

1. Asset Managment

1. University owned equipment and software will have a responsible party and be indexed by University asset tags and/or serial numbers.
2. Systems and network equipment will be classified based on the type of data it contains, availability requirements for the services they offer and how critical they are to operations.
3. University owned devices capable of attaching to the Unified Active Directory Domain (Windows) or Casper (OS X) will do so.

2. Account Administration

1. Accounts should only given to current student, faculty, staff, alumni, and sponsored affiliates.
2. User accounts will come from UA Unified Active Directory with authorization based on group or role based access rights assigned to an individual.
3. Guest account will be set to expire when expected activity is completed.
4. Account inactivity and/or removal periods will be established and documented.
5. Accounts will be protected at a minimum with passwords.
6. Accounts with administrative rights have higher standards for protection applied to them.
7. Account sharing is not permitted with the exception of documented and required shared service accounts in support of automated business operations.
8. Accounts will lock after a specified number of failed access attempts.

3. Password

1. Passwords will conform to, at minimum, NIST LOA2.
2. Passwords expiration will be set to, at most, 400 days.

4. System security patches or updates and security mechanisms

1. Systems and software will be patched/updated at least quarterly with routine patches/updates to keep software current.
2. Security related patches/updates will be applied within 5 business days of release after completion of testing.
3. Security patches/updates for exploits in the wild will be patched within 48 hours after completion of testing.
4. Where systems can not be patched due to negative impact to business operations a

Plan of Action & Mitigations report will be presented to the appropriate ISO.

5. Encryption and authentication

1. Only secure authentication methods will be used.
2. When sensitive data is exchanged encrypted transfer protocols will be used.
3. 128 bits encryption keys are the minimum acceptable length and Advanced Encryption Standard (AES) will be the preferred algorithm unless it is not an available option.
4. 256 bit encryption keys are recommended.
5. Systems storing data classified as “Restricted” in the UA Data Classification schema will be stored on encrypted media.

6. System/Network Services

1. System administrators will disable unused/needed system/network services.
2. System administrators will define and implement compensating controls system/network services they determine are risky or vulnerable.
3. Services will only be made available to their target audience.

7.Logging

1. Systems and software will log all security events, authentication and authorization events to a centralized log repository not on the system they were generated on.
2. Logs will be kept for a minimum of 180 days and a maximum of 3 years unless otherwise required by law, applicable regulation or funding agency.

8. Monitoring

1. Each major unit or department should monitor the network and systems for abuse and intrusion within their span of control.
2. Abuse or intrusions (including malware) should be reported to the UA CIRT group through the appropriate Information Security Officer.

9. Physical Security

1. Systems used by individuals will be secured by physical restraints in their primary work area when unattended.
2. Server and networking equipment will reside in a secured, limited access space.
3. Critical systems or devices or those containing Restricted data will reside a server room managed or approved by a major unit IT department.

10. Acceptable Use

1. Enterprise or workgroup assets, not individuals’ workstations, will not be used for incidental personal use.
2. Individuals’ workstations will not be used to provide enterprise or workgroup services.

11. Network Access Controls

1. Layers of network access controls will be used to scope access appropriately.

2. Access controls will deny by default all unsolicited access with the exception of declared ports and protocols.
3. Hosts will utilize host based firewalls as a second layer.

12. Special Controls

Where there are special security requirements that exceed the level of security provided in the controls above they need to be documented and observed. Examples of this would be resources covered by special regulation or funding agency requirement. Please contact security@alaska.edu with the special considerations, the resources covered, a point of contact for the resources and a statement of what security services the system owners/operators are relying on central IT service providers to provide in terms of security.

13. Risk Assessment

1. Risk assessments will be conducted and documented prior to IT system implementation for management review.
2. Assessments will be affirmed or updated at least annually.
3. Significant* changes to IT systems should trigger a reassessment.

14. Incident and Breach Notification

1. Campus ISOs will be notified of all incidents and/or suspected breaches in accordance with the Information Security Breach Notification procedure at the campus.
2. Campus ISOs will notify OIT Security Oversight Services of all breaches and include an assessment of impact.

15. Data Sanitization

1. Internal or removable storage media leaving physical control of the organization needs to be sanitized with a multi pass algorithm.
2. Media that is not functional for sanitization needs to be physically destroyed.
3. Flash based media needs to be physically destroyed as multi pass sanitation does not work on this media.

* Significant changes are defined as those that add new functionality or fundamental alteration of existing functionality. Some examples might be enabling a previously unused file transfer protocol or using different software to provide a services. Creation of a system or service is always a significant change.