UNIVERSITY
of ALASKA
Many Traditions One Alaska

Accounting and Administrative Manual

Section 400: Information Technology

Information Technology: Security Program	Date: 11/8/22
No.: 400: A-01	Page: 1 of 5

University of Alaska Information Security and Assurance Program

1.0 Overview and Purpose

The University of Alaska System is subject to a variety of regulatory and contractual compliance requirements related to the collection, processing, and sharing of data, including personally identifiable information, and the provisioning of accounts and/or services to its customers and partners.

The purpose of the UA Information Security and Assurance Program is to promote an overarching strategy for compliance with the numerous legal and policy requirements that apply to UA operations. The purpose of this document is to provide an overview of the administrative, technical and physical safeguards in a readily accessible place.

2.0 Applicable Board of Regents Policies

P02.02.070 (Chief Information Technology Officer) establishes that the responsibilities of the CITO includes ensuring the security of the core information systems, coordinating the development and implementation of IT standards, and coordinating the planning and adoption of best practices in the management of information technologies and services.

P02.07.060 (Protection and Enforcement) requires UA to "establish procedures for securing its information resources against unauthorized access or abuse to a reasonable and economically feasible degree."

P02.07.066 (Mobile Device Security) charges the CITO with "coordinating with the campuses in the development of consistent measures and business practices for ensuring security of non-public data on mobile devices."

P02.07.070 (Administrative Responsibilities) allows each university to "define rules and enforcement mechanisms for use of information resources under its control" provided that they are consistent with Policy and Regulation.

3.0 Qualified Individual

3.1 Designation

The UA Chief Information Technology Officer (CITO) has delegated management, implementation and oversight of the Information Security and Assurance Program to the UA Chief Information Security Officer (CISO, also referred to as the "Qualified Individual" pursuant to 16 CFR 314.4(a)). The CISO serves as ex officio member of the UA CIO Management Team (CMT) alongside the CITO and the senior IT leader from each university. The CISO raises security issues to the CMT and provides expertise to guide their decision-making.

3.2 Enforcement

The CISO is responsible for coordinating with the senior IT leader at each university in the enforcement of security standards. In situations where coordination is not practicable, the CISO is empowered to take direct measures to protect university systems and data, with notice to and coordination with impacted universities as soon as possible.

4.0 IT Risk Management

The CISO oversees IT risk management activities in coordination with the CMT and Enterprise Risk Management. The IT risk management program identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of UA information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks. Risks are ranked according to the impact and likelihood after mitigation and this ranking is used to develop safeguards and prioritize resource allocation.

5.0 Safeguards Against Known Risks

5.1 Data Classification Standard

5.2 Data Encryption, Retention, and Destruction (at rest and in transit, including media protection)

5.3 Digital Identity Management (role-based access controls, privileged access, and multi-factor authentication)

5.4 Employee Control (on-faff-boarding, position control, separation of duty management)

5.5 Host-based controls (antivirus, antimalware, endpoint detection/response, host-based firewall, application control, device control, file integrity monitoring)

5.6 Network and Boundary Design and Protection (incl. posture checking/enforcement), virtual private networking, and next generation firewall design and administration

5.7 Patching and Vulnerability Management

5.8 Physical Security (incl. visitor and contractor management)

5.9 Secure Development Standards

6.0 Monitoring and Testing

UA combines both continuous monitoring as well as periodic intrusion testing and vulnerability scans. Identified vulnerabilities are shared with system administrators (per R0l.07.074) for remediation.

7.0 Training, Qualifications, and Currency

Security awareness training is provided to all employees and is required annually for employees identified as having access to certain high risk data or services. Training materials are updated as necessary to reflect risks identified by the risk assessment. Program personnel are provided training and professional development opportunities at least annually to ensure currency of knowledge. The CISO is responsible for ensuring Program staff are qualified to manage Program activities and address relevant security risks.

8.0 Third-Party Service Providers

UA business units are required to coordinate with Procurement prior to purchasing any IT-related systems or services and should complete the "Saas Checklist" as soon as practical, but in all cases before any production use of such services has commenced or UA Data has been shared. The Program conducts risk assessments at the request of Procurement for new purchases and contract renewals.

Pursuant to the "Data Security Addendum", service providers are required to promptly inform UA of any breach to their systems involving UA data and are not permitted to share, transfer, or sell that data or derivative works to others without UA's explicit written permission.

9.0 Continuous Improvement

Elements of the Information Security and Assurance Program are continuously reviewed for efficacy and relevance to the UA System and to the threats targeted to the system and its customers. Material changes to the Program are reviewed and approved by the CISO in collaboration with the CIO Management Team and are noted in this document and/or reported to the Board of Regents at least annually.

10.0 Incident Response

UA routinely engages in proactive threat assessment to minimize the risk of security incidents. When incidents occur, UA has defined procedures and standards related to incident handling and response.

Employees, students, or affiliates who suspect they have identified an information security incident should promptly contact UA Information Security at 907-450-8370 (24/7 Data Center Operations) or ua- oit-security@alaska.edu to report any relevant details related to the incident.

11.0 Reporting

The CITO provides an IT report at each regular meeting of the BOR Facilities and Land Management Committee meeting. In addition, the CISO prepares an annual security report for inclusion in the board packet.