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 Prograand/or

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.

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-

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.