INFORMATION SECURITY STANDARD

Effective Date: July 11, 2018
Last Revised: August 19, 2022

INFORMATION TECHNOLOGY RISK ASSESSMENT

Northern Arizona University owns or controls, and acts as custodian for, a broad array of information, including Highly Sensitive Information protected by law. Maintaining the integrity and availability of this information is an important University function. To this end, Information Security Services deploys a comprehensive framework of *Information Security Standards* of which this document is a part. All members of the University community are required to comply with these requirements. Capitalized terms used herein are defined in the *Information Security* policy or *Data Classification and Handling* policy. Questions regarding the *Information Security Standards* should be directed to Information Security Services.

In the interest of proactively mitigating system vulnerability or exposure, this Information Security Standard establishes standardized University Information Technology ("IT") risk assessment requirements and procedures.

1. **Scope**. All University IT Resources, and especially those that handle Sensitive and/or Highly Sensitive Information, provide network connections, or function as part of authentication, authorization, and access control systems shall be reviewed periodically to identify areas of IT risk across the University. IT risk assessment is a continuous cycle of improvement that includes the following:

    - Developing and maintaining an IT risk assessment survey or tool (in some cases, a third party may perform an IT risk assessment or provide a survey or tool)
    - Periodically distributing the IT risk assessment survey or tool, typically annually
    - Analyzing responses
    - Identifying areas of IT risk across the University through a variety of efforts, including the NAU Enterprise Risk Management Oversight Committee processes and NAU Internal Audit's audit planning processes
    - Reporting risk assessment results to leadership as appropriate
    - Identifying corrective actions
    - Corrective action planning, development, implementation, assessment, and reporting
    - Enforcing corrective actions as necessary

2. **IT Risk Assessment Roles and Responsibilities**.

    - Chief Information Officer ("CIO"): establishes, maintains, and revises as necessary the IT risk assessment survey or tool and authorizes third-party risk assessment engagements. Communicates with the Data and IT Governance Trustees and the Enterprise Risk Management Oversight Committee ("ERMOC"), as needed, and approves corrective action plans.

    - Data and IT Governance Trustees: provides communication and endorsement of the IT risk assessment process to business units and assists Information Security Services in identifying appropriate survey respondents. Approves corrective action plans.

    - Director of Information Security Services: as authorized by the CIO, develops, maintains, and conducts IT risk assessments, analyzes responses, reports to the Data and IT Governance Trustees and the ERMOC regarding risks and corrective action plans, and works with risk assessment survey respondents. Coordinates with NAU Internal Audit as related to developing the periodic / annual Internal Audit plan and in planning and addressing IT risk matters identified in specific Internal Audit projects.

- The ERMOC: advises on risk assessment frameworks and processes and performs analysis and reviews of completed IT specific assessments. Identifies and prioritizes IT risks based on completed assessments and reviews and provides guidance on proposed corrective actions to mitigate the most significant risks facing the University.

- Information Technology Risk Assessment Survey Respondents: business unit liaisons designated by the Data and IT Governance Trustees, dean, or department head who provide responses to IT risk assessment surveys or tools and assist with the deployment of corrective action plans.

3. **Assessment Survey or Tool**. Risk assessment surveys or tools will include assessment attributes (often in the form of questions) derived from industry best practices and applicable standards, such as the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, NIST risk assessment guide, Educause Risk Registers, and the Committee of Sponsoring Organizations ("COSO"). The survey or tool may include Likert scale ratings, maturity level selections, multiple choice, checkbox selections, open-ended questions, and/or respondent feedback opportunities. Assessment attributes and possible responses will be reviewed and approved by the CIO and the Director of Information Security Services and tested within the Information Technology Services department to gauge effectiveness and identify any need for refinement or elaboration prior to wider distribution. The review process may include small group discussions, presentations, or question and answer sessions as well as email feedback.

4. **Communication and Distribution**. IT risk assessments will be communicated to all business units involved and to the Data and IT Governance Trustees prior to distribution. Distribution of the survey or tool will begin with Information Technology Services leadership and management teams, followed by business units with internal IT support staff. The survey or tool will then be distributed to the designated survey respondents in academic and administrative units. The IT risk assessment process shall be announced by the Data and IT Governance Trustees and senior management, and assessment results will be communicated to the ERMOC.

5. **Analysis and Reporting**. Analysis of IT risk assessments will be performed by the Director of Information Security Services in order to summarize the results and document prioritized risk areas requiring remediation. Initial rankings and degrees of risk, remediation, and corrective actions shall be performed and then reported to the CIO. Results shall be shared with the University's Chief Audit Executive while the ERMOC shall evaluate overall impacts, challenges, and opportunities to identify the top risk areas needing corrective action plans.

6. **Corrective Action Plans**. The ERMOC will identify and reach agreement on the uppermost risks during the risk assessment analysis phase and shall ensure corrective or mitigating actions or measures have been developed and are being implemented in response to the aggregate IT risk assessment results. Mitigation plans to include deployment timelines will be created for departmental implementation. As appropriate, risk mitigation plans and recommendations will be transmitted to the CIO and to the Data and IT Governance Trustees for confirmation and approval. Corrective actions may include but are not limited to:

    - Information Security Awareness training for University Community Members
    - Presentations or tailored training for specific department and business unit needs
    - Business unit consultation to identify existing service or resource gaps
    - Improvement, configuration, or provisioning of services and resources, including the potential for centralizing services
    - Application of compensating controls authorized by the Data and IT Governance Trustees
    - Coordinating with NAU Internal Audit to audit or review the implementation of corrective actions to ensure related controls are addressing the risks as intended.

Following approval of corrective action plans by the Data and IT Governance Trustees, Information Security Services will contact business units to discuss key mitigation plan elements, such as implementation timelines, testing methods, and progress reporting mechanisms.