NAU INFORMATION SECURITY STRATEGIC PLAN

2022 - 2024

INTRODUCTION AND MISSION

Northern Arizona University is committed to ensuring the security, availability, confidentiality, and integrity of its information technology (IT) resources. The NAU Information Security Program has an established governance structure to continually monitor and improve upon services, establish measurements of success, and assess the Program to illustrate Program effectiveness or identify areas needing improvement. NAU follows a risk-based approach to meeting its security goals and objectives.

The Information Security Program has a well-established set of goals, objectives, and areas of focus. The following objectives represent the primary focal points and objectives of the Program for the 2022 - 2024 time frame. Additionally, the Program will provide annual reports illustrating metrics used for assessing the Program.

INFORMATION SECURITY OBJECTIVES

The NAU Information Security Program has the following goals, objectives, and areas of focus. Program effectiveness will be measured on progress shown, or not shown, towards the achievement of these goals, objectives, and areas of focus, as well as an annual IT Risk Assessment / Maturity Rating process.

- Develop, review, update and disseminate information security policies, standards, procedures and practices.
- Align to the NIST Cybersecurity Framework as a framework that unifies information security policies, standards, processes and procedures with the University's strategic goals and initiatives.
- Ensure the confidentiality, integrity, and availability of the University's information and IT resources.
- Raise information security awareness by educating the NAU community on best practices for securing data and information resources from damage, modification, loss, and unauthorized access.
- Integrate IT General and IT Security Controls into business processes by collaborating with college and department leaders, project managers and business process owners.
- Assess and manage information security risks.
- Detect and rapidly respond to security events and incidents.
- Continually improve upon and monitor services, establish measurements of success, and assess the Program to illustrate effectiveness of the Program or to identify areas needing improvement.
- Update NAU leadership on pertinent information security matters.

The following objectives represent the primary areas of focus for the Program in 2022 - 2024:

Objective 1: Increase information security awareness across Northern Arizona University.

Objective 2: Maintain a strong risk management program through the continuous technology risk assessment process.

Objective 3: Improve and grow the data classification and handling program.

Objective 4: Enhance the university's information security logging and monitoring, vulnerability assessment, and web application penetration testing.

Objective 5: Enhance the University's authentication mechanisms to protect users and IT resources while modernizing existing systems, access controls, and services.

NAU Information Security Strategic Plan

2022 - 2024

Objective	Metric	Current Progress	Target Metric
1 - Increase information security awareness across NAU	Percentage of Faculty and Staff trained annually	86%	100%
2 - Maintain a strong risk management program through the continuous technology risk assessment process	Percentage of IT Departments completing periodic IT Risk Assessment and corrective action plan	100%	100%
3 - Improve and grow the data classification and handling program	Percentage of Departments completing periodic data classification and activity mapping	99%	100%
4 – Enhance the monitoring and management of… a) The university's information security logging and auditing b) Scanning and monitoring for patch-related or configuration related vulnerabilities c) Penetration testing of risk web applications	Percentage of… a) High risk resources meeting NAU logging standards b) High risk systems scanned for vulnerabilities c) High risk web applications tested for vulnerabilities	a) 80% b) 90% - *see description for more details* c) 40%	In all cases: 100% of those classified high-risk
5 - Enhance the University's authentication mechanisms to protect users and IT resources while modernizing existing systems, access controls, and services.	Percentage of current and active University Community Members protected by two-step verification	98%	100%

Objective 1: Increase information security awareness across NAU

Description: All authorized users should gain a broad understanding of information security threats, risks, and best practices in order to assist the University in protecting the integrity of University Information and the University's Information Technology ("IT") Resources. NAU offers a series of training modules online as well as in-person presentations and focused-details for specific populations of users.

FY20 and FY21 Accomplishments	NAU continued to maintain an established information security essentials training program. In person trainings and presentations included Two-Step Verification and risk management, as well as encryption best practices, to groups including the Information Security Committee and Faculty Senate. Critical Messaging was used for those not completing the training and the percent of completion went from 80% in July 2019 to 86% in July 2021. A Department of Homeland Security, DHS, Award was obtained for testing of a vendor platform and Proofpoint was used for web-developer training as well as Phishing Simulations in the ITS Department. Workshops were provided to groups around campus, webisodes created for National Cyber Security Awareness Month, and a 2021 Data Inventory Interview process allowed for awareness raising to 140 business units around Data Security.
Plan for FY22	NAU will continue to enhance the information security training program with newly updated training modules, seeking to use vendor supplied relevant and up to date topics. Additionally, the vendor platform will provide greater opportunities for Phishing Simulation to users in order to raise awareness around identifying and reporting suspicious email. In-person and virtual, live and recorded, presentations to campus units will be scheduled and performed.

Objective 2: Maintain a strong risk management program through the continuous technology risk assessment process

Description: NAU follows a risk-based approach to information security. Risk challenges and opportunities are assessed at an enterprise level, within the framework of an enterprise risk management model. Information technology and information security risk assessment processes will be used to identify key risk areas and then define methods to mitigate the risk challenges and optimize the risk opportunities.

FY20 and FY21 Accomplishments	Enterprise Risk Management (ERM) interviews were conducted with executive and cabinet levels to document risks, challenges, and opportunities facing NAU in all areas. Annual IT Risk Assessment process was followed for the second and third time, resulting in risk identification and reporting to the ERM Oversight Committee and the IT and Data Trustees.
Plan for FY22	ERM data will be compiled and a new process in which Strategic Roadmap alignment and creation of risk appetite statements and risk tolerance levels will be implemented. The IT focused risk assessment survey will be conducted again in Fall 2022 to assess changes and trends and to help identify where people, process, or technology risks and threats exist so that strategic planning on their remediation can be performed. Results from both efforts – ERM and IT Risk Assessment – will work to inform action plans.

Objective 3: Improve and grow the data classification and handling program

Description: The unauthorized release of sensitive information can inflict substantial financial and reputational harm to NAU. Therefore, maintaining the integrity of this data and the information systems where it is stored is a fundamental obligation. All members and units of the NAU community that interact with sensitive data should have clear standards and protocols for ensuring its integrity, confidentiality, utility, and availability. Data classification and handling processes will be implemented to support the NAU Community in protecting data.

FY20 and FY21 Accomplishments	A Data Classification policy and accompanying set of data handling protocols was reviewed, revised, and published. Communications were made to a group of key stakeholders and data owners. A data inventory was conducted via questionnaires in FY20 and expanded to include 140 unit interviews in FY21. This effort led to raising awareness around Data Classification and Handling, Data Protection and Security, and the creation of an initial Data Inventory showing systems and software handling or storing the different levels of data types.
Plan for FY22	A project exists to continue compiling data from the recent interviews and schedule follow-up interviews with data owners who handle the most sensitive data types. Interviews will involve assisting the respondents with formal documentation of their data inventory and protection plans. Annual follow-ups will be scheduled to review changes to inventory, uses, and progress made on corrective action plans.

Objective 4: Enhance the monitoring and management of…

a) The university's information security logging and auditing
b) Scanning and monitoring for patch-related or configuration related vulnerabilities
c) Penetration testing of high-risk web applications

Description: NAU has developed and implemented a comprehensive scanning and monitoring model to provide greater insight, visibility, and situational awareness into the network, systems, and anomalous user activities. These approaches include steps to improve visibility into potential weaknesses and inappropriate uses of IT resources. Continuously logging, monitoring and scanning for these helps improve the overall security posture of NAU in order to detect, and protect against, and remediate damage that may have been caused by malicious activities.

FY20 and FY21 Accomplishments	Development and implementation of Information Security policies and standards. Continued the engagement with DHS for third party network scanning and a separate engagement with the University of Texas for third party web-application scanning. Automation of several steps involved with the Vulnerability Management program was completed, and increased forwarding of system logs to Splunk for visibility and alerting was another accomplishment during this time.
Plan for FY22	Continue to improve the coverage of scanning capabilities to assess systems identified as critical or high-risk. Continue to engage with third parties to obtain external-view of security posture and weaknesses visible to the world in order to reduce risks and likelihood of attacks, and improve the frequency and number of high risk systems and applications receiving penetration testing. Increase log correlation capabilities and alerting for faster detection of information security incidents.

Objective 5: Enhance the University's authentication mechanisms to protect users and IT resources while modernizing existing systems, access controls, and services.

Description: Phishing and attempts to steal user credentials remains one of the top threats to data integrity, and NAU is no exception to these attempts. One method to mitigate loss or misuse from stolen credentials is strong passwords – another, more effective method, is the use of two-step verification or multi-factor authentication. Verifying a user identity using modern authentication methods prevents an attacker from logging in. Therefore, increasing the use of modern authentication, including two-step verification, where sensitive and very sensitive data usage occurs protects the user and the university, as well as the people for whom NAU collects and maintains data.

FY20 and FY21 Accomplishments	High risk departments and applications were identified and ranked for prioritization. The roll-out to several departments was executed, including HR/Payroll, Student Financial Aid, Registrar Office, NAU Police Department, and ITS. Additional phases of enrollment was planned and executed, such as the Virtual Private Network (VPN) for all users of that service; Office 365; NAU CAS protected applications; and Full time employees in Spring 2021, followed by all students in Fall 2021.
Plan for FY22	Look to identify options for modernizing the overall Identity and Access ecosystem by engaging with outside party to assist in performing as-is review, future-state options, and paths to achieving them (vendor platform or open source InCommon approach). Look to modernize the authentication mechanisms using the NIST 800-63 standards.