Responsible Executive: Chief Information Officer
Responsible Office: Information Security Services
Effective Date: February 13, 2018
Last Revised: August 19, 2022

DATA CLASSIFICATION AND HANDLING

POLICY SUMMARY

Northern Arizona University owns or controls, and acts as custodian for, a broad array of information, including information protected by law. Because the unauthorized release of protected information can inflict substantial harm, maintaining the integrity of this data and the information systems where it is stored is a fundamental obligation. This policy establishes a data classification structure and data handling protocols to support this crucial task. All units and University Community Members that interact with data must comply with the requirements of this policy.

REASON FOR THIS POLICY

Clear standards, requirements, and protocols for the identification, classification, and internal handling of University information are an important contributor to the goal of maintaining its integrity and availability.

ENTITIES AFFECTED BY THIS POLICY

- All units that handle or interact with University information or data
- External Data Use Committee
- Information Security Committee
- Information Security Services
- NAU Communications

WHO SHOULD KNOW THIS POLICY

- All University Community Members who interact with University information or data
- Chief Information Officer ("CIO")
- Chief Institutional Data Officer
- Data Stewards
- Data Governance Trustees
- Director, Information Security Services

DEFINITIONS

Data Steward: an official charged with controlling access to and properly curating University information or data.

Data Cookbook: an electronic library housing data element metadata and other information.

University Community Member: all University faculty, staff, student employees, students, alumni, affiliates, contractors, consultants, agents, and volunteers wherever located.

POLICY

A. Data Identification and Classification

All units and University Community Members shall identify and classify University information or data using the definitions described herein. Data identification must include the information systems used to handle and store

the data, and special care must be given to data classified as Sensitive or Highly Sensitive. All University information or data generated, processed, transmitted, or otherwise handled, regardless of how the data is stored, the media or systems used to process it, or the systems or methods by which it is accessed or distributed, must comply with the Data Handling Protocols. Questions regarding data types and how best to protect them should be directed to the appropriate Data Steward, the Chief Institutional Data Officer, or Information Security Services.

Level 1 Public Data – Very Low Risk

Level 1 Public Data is generally publicly available and intended for public use. This information may be freely distributed to the general public, all units, and University Community Members, as there is no concern of unauthorized disclosure with Public Data. Access controls are necessary, however, to help protect Public Data integrity. See the *Data Type Examples* tool for examples of Level 1 Public Data.

Level 2 Internal Data – Low Risk

Level 2 Internal Data is not generally available to the public or to parties unaffiliated with the University. Risk of disclosure and harm to the University or University Community Members is low, however, as little or no adverse effects on the University's operations, assets, reputation, financial position, privacy obligations, or the personal privacy of individuals could result. See the *Data Type Examples* tool for examples of Level 2 Internal Data.

Level 3 Sensitive Data – High Risk

Level 3 Sensitive Data is private information intended for restricted use within the University. Access to Sensitive Data is limited to protect its integrity and confidentiality. A high level of risk is associated with these data types and they must be protected from unintended or unauthorized disclosure, loss, or destruction. Unauthorized release of Sensitive Data could have substantial and costly negative effects to the University or to University Community Members. Unauthorized exposure or loss of Sensitive Data could contribute to fraud, identity theft, legal violations, and substantial reputational, financial, or operational damage. See the *Data Type Examples* tool for examples of Level 3 Sensitive Data when stored or released separately from other personally identifiable information.

Level 4 Highly Sensitive Data – Very High Risk

Level 4 Highly Sensitive Data is the most confidential and sensitive data possessed or controlled by the University. Level 4 Highly Sensitive Data must be protected with the highest levels of security that are reasonably attainable. Highly Sensitive Data is intended for extremely limited use consistent with substantial legal requirements for its protection and stewardship. Any unauthorized access, disclosure, compromise, loss, modification, or destruction of Highly Sensitive Data could result in severely negative impacts or damage to the University, to University Community Members, or to independent entities that may have provided the data. As with Sensitive Data, the unauthorized exposure or loss of Highly Sensitive Data could cause or contribute to fraud, identity theft, financial loss, substantial reputational damage, and even physical endangerment that creates safety risks for individuals. For these reasons, the University prohibits the transmission of this data via electronic mail. See the *Data Type Examples* tool for examples of Level 4 Highly Sensitive Data.

Please note: contact the Office of the Vice President for Research with any inquiry regarding the classification or handling requirements for information or data related to research or External Data Use Agreements.

B. Data Sharing Requirements

Data from a given classification may only be shared with University Community Members who have completed the training necessary to be granted appropriate access and authorization to that data. If it is necessary to provide data to an individual without the appropriate clearance, the Data Steward, Data Trustee, or Chief Institutional Data Officer may approve the data sharing in advance and in writing, provided that the receiving official displays the requisite awareness of, commitment to, and ability to comply with the applicable Data Handing Protocols. The transmittal of data to any non-University third-party must be approved in advance and in writing by an authorized University official. All data requests will be reviewed by the appropriate University unit or official prior to approval and must include an evaluation of appropriate data security controls. Research and service projects often involve data owned/controlled by both NAU and external partners. The handling of

external research or service data by University officials must take place in accordance with any applicable Material Transfer Agreement, Data Use Agreement, or other agreement as outlined further in the External Data Use Agreements policy.

C. Data Handling Protocols

The CIO, with the concurrence of the Chief Institutional Data Officer, shall establish, update, revise, and republish, as necessary and appropriate, a comprehensive set of protocols designed to maintain the integrity, security, confidentiality, control, and availability of the University's data and information systems. These *Data Handling Protocols* shall be based on the sensitive data type classifications established herein and shall promote data handling best practices and compliance with all applicable laws, regulations, policies, and contractual or licensing requirements. Data element metadata, including the data element's sensitivity classification, shall be recorded and maintained in the Data Cookbook information system of record. These protocols shall cover, at a minimum, the following:

1. Access Controls
2. Copying/Printing
3. Network Security
4. System Security
5. Electronic Mail
6. Physical Security
7. Remote Access
8. Storage
9. Transmission
10. Backup and Disaster Recovery
11. Data Destruction and Disposal
12. Training

D. Applicability and Implementation

This policy governs all data and information systems and devices owned by the University or utilized for University business. The policy applies to all campuses, units and University Community Members wherever located. On an annual basis, each unit will classify all data within its care and implement the appropriate data handling protocols. All units and University Community Members will use the sensitive data classifications established herein to determine the appropriate data handling requirements as outlined in the *Data Handling Protocols*.

E. Mandatory Reporting

All University Community Members are obligated to immediately report any IT security threat suspected or actual release or breach of Sensitive Data or Highly Sensitive Data. **Dial 928-523-3335 to make a report**. In collaboration with appropriate University stakeholders, Information Security Services is responsible for notifying all affected and responsible parties. The CIO will assemble an incident response team to investigate, preserve evidence, mitigate the situation, and analyze and report on the event. If health or safety may be a concern, the reporting party or Information Security Services shall immediately notify the Northern Arizona University Police Department and any other external entity or governmental agency as appropriate.

F. Public Records Requests

Data classification in accordance with this policy does not alter public information access requirements or the University's need to fulfil other legal obligations that may require the disclosure or release of information from any of the classification levels established under this policy. Questions regarding public records requests should be directed to NAU Communications or the Office of General Counsel.

G. Compliance and Enforcement

As outlined in the University's *Information Security* policy, when necessary to protect the integrity or security of its IT Resources or information systems and the University Information they contain, the University may suspend access to its networks or devices and may examine any user account. At the discretion of the CIO, enforcement

of this and related IT policies may include the removal of devices or systems from the University's information networks until compliance with applicable requirements is achieved. Violations by a University Community Member of the duty and responsibility to protect the University's data, IT resources, and information systems in accordance with this and other applicable policies, standards, or requirements may also result in denial of access to University Information and/or University IT Resources or the temporary or permanent revocation of access privileges. Individuals who violate this policy are subject to disciplinary action under applicable Arizona Board of Regents and University conduct policies up to and including expulsion or termination and possible civil liability or criminal prosecution. In cases where full compliance with the requirements of this policy may not be immediately achievable, the unit's leadership must consult with Information Security Services to develop a plan for achieving compliance as soon as possible.

RESPONSIBILITIES

Chief Institutional Data Officer: in collaboration with the Chief Information Officer, update as necessary and appropriate the University's *Data Handling Protocols* and train the University community in proper use of the Data Cookbook.

Chief Information Officer: in collaboration with the Chief Institutional Data Officer, update as necessary and appropriate and support the Director of Information Security Services with enforcement of this policy and the *Data Handling Protocols*.

Data Stewards: evaluate requests for data or information system access to determine if request is appropriate and justified based upon an employee's role and responsibilities.

Director, Information Security Services: develop and implement security policies, procedures, protocols, and standards in support of this policy and the Information Security Program; is the primary enforcer of this policy and the *Data Handling Protocols*; serve as chair of the Information Security Committee.

External Data Use Committee: assist all units and University Community Members—primarily faculty members and research administrators—in initiating, negotiating, and maintaining compliance with External Data Use Agreements as established in the *External Data Use Agreements* policy; work to ensure that the handling of external research or service data takes place in accordance with applicable Data Use Agreements, as outlined further in the *External Data Use Agreements* policy.

NAU Communications: coordinate the University's response to public information requests that implicate Level 2, 3, or 4 data with affected units as appropriate.

System Administrators and Technicians: maintain the privacy and confidentiality of sensitive information seen or obtained in the normal course of their work, and report suspected or actual violations of the University IT policies to the appropriate University authority.

University Community Members: ensure the effective implementation and enforcement of this policy within their respective areas of responsibility or jurisdiction.

PROCEDURES

There are no procedures associated with this policy.

RELATED INFORMATION

Forms or Tools

Data Handling Protocols

Data Type Examples

Northern Arizona University Data Cookbook

Cross-References

Appropriate Use of Information Technology Resources

Electronic Mail

External Data Use Agreements

Information Security

Sources

Arizona Board of Regents Policy 9-201

Arizona Board of Regents Policy 9-202

Arizona Revised Statues § 44-1373. Restricted use of personal identifying information

Arizona Revised Statutes §15-1823. Identification numbers; social security numbers

Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99)

Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191)

Gramm-Leach-Bliley Act (Public Law 106-102)

APPENDIX

None.