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

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 m

Northern Arizona University Data Cookbook

Cross-References

Appropriate Use of Information Technology Resources