

---

## DATA HANDLING PROTOCOLS

In accordance with Northern Arizona University's [Data Classification and Handling](#) policy, the Chief Information Officer ("CIO") and Chief Data Officer ("CDO") maintain the data handling protocols set forth below. These data handling protocols are based on the University's four data classifications:

### **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.

### **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 Level 3 Sensitive Data, the unauthorized exposure or loss of Level 4 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.*

## **Identifying and Classifying University Information and Data**

All units and University Community Members, including all faculty, staff, students, alumni, affiliates, contractors, consultants, or agents, wherever located, must identify and classify all University information or data in their care and implement the appropriate data handling protocols, as outlined below. Contact the appropriate Data Steward, the Chief Data Officer, or Information Security Services with questions about data classification and handling and the best means of protection.

## **Data Dictionary System of Record**

The university maintains a Data Dictionary for recording metadata about data. The Data Dictionary element metadata, including the data element's sensitivity classification, shall be recorded and maintained in the Data Dictionary system of record.

The Data Dictionary records for classified data shall include:

- The classification level
- The system of record for the data
- The data steward (by position or name)
- Associated compliances (FERPA, GLBA, HIPAA, etc)
- Reviewers Email (typically the data steward)
- Last Reviewed/Updated By
- Last Reviewed/Updated Date

Data Cookbook is the Data Dictionary system of record.

## **Periodic Reviews**

Elements of the Data Dictionary shall be reviewed annually by the designated reviewer (typically the assigned data steward).

- The Offices of the CIO and CDO will oversee the annual review of data elements.
- Taking a risk-based approach, the priority is to review Level 4 and Level 3 classified data.
- Annually, the data stewards will be prompted to review for accuracy, the data assigned to them using established mechanisms of the data dictionary.
- Data stewards will identify any missing or new data and complete one or more established workflows to update data metadata in the data dictionary system of record and record their review of data elements.
- The CIO and CDO or their designees will report annually to the IT and Data Governance Trustees regarding review process and status of the Data Dictionary.

## **Data Handling Protocols**

In accordance with Northern Arizona University's Data Classification and Handling policy, the Chief Information Officer ("CIO") and Chief Data Officer (or their designees) will, at least annually, review and update the data handling protocols set forth below:

These data handling protocols represent minimum baseline standards for the protection and secure handling of university information or data. Additional controls may be necessary or advisable in special circumstances, such as when a data type is governed by applicable laws or regulations (e.g., health, financial, or research information). Contact the CIO, the CDO, or Information Security Services with any inquiry or feedback regarding these protocols.

If minimum baseline standards cannot be met, the owning Data Steward may request an exception with ISS. This request should include:

- Why the standard cannot be met
- What risk mitigations have you put in place
- What other options have you explored

Exceptions may be granted after a consultation on a case-by-case basis.

In the tables below—

- “No Restrictions” means the data can be publicly disclosed without limitations;
- “Encouraged” means the data should remain confidential when possible but that such confidentiality is not required;
- “Required” means the data must remain confidential in accordance with all applicable laws, regulations, policies, and/or contractual obligations. Exceptions may be granted on a case-by-case basis with the approval of the CIO or their designee; and
- “Mandatory” means that maintaining the data’s confidentiality in strict adherence to all privacy and security protections as set forth in all applicable laws, regulations, policies, and/or contractual obligations is mandatory. Exceptions may NOT be granted by NAU alone but may be approved in conjunction with other external parties on a case-by-case basis.

<b>Access Controls Data Handling Protocol</b>	<b>Level 1 Data</b>	<b>Level 2 Data</b>	<b>Level 3 Data</b>	<b>Level 4 Data</b>
Open access to public information	No Restrictions	Mandatory	Mandatory	Mandatory
Viewing and modification restricted to authorized individuals	No Restrictions	Mandatory	Mandatory	Mandatory
Access granted at discretion of, and by, data owner, Data Steward, or designee in addition to approval from supervisor	Required	Required	Required	Required
Authentication and authorization required for access, using username and strong password	Required for modification only	Required	Required	Required
Two-Step Verification and authentication	No Restrictions	Encouraged	Encouraged	Required
Access lists should be reviewed periodically to ensure that access is still needed	No Restrictions	No Restrictions	Required	Required
Human subject research data requires Data Use Agreement Committee/Institutional Review Board approval	No Restrictions	No Restrictions	No Restrictions	Required
Persona Accounts that are utilized for accessing on-premises resources are required to be on NAU authorized networks	Required	Required	Required	Required

<b>Backup/ Recovery Data Handling Protocol</b>	<b>Level 1 Data</b>	<b>Level 2 Data</b>	<b>Level 3 Data</b>	<b>Level 4 Data</b>
Daily backups to a CIO's, or their designee's - approved solution	Required	Required	Required	Required
Encryption of backups	No Restrictions	Required	Required	Required
Off-site storage	No Restrictions	Encouraged	Required	Required
Backups should be tested periodically	Encouraged	Encouraged	Required	Required

<b>Copying/Printing Data Handling Protocol</b>	<b>Level 1 Data</b>	<b>Level 2 Data</b>	<b>Level 3 Data</b>	<b>Level 4 Data</b>
Printing data	No Restrictions	Mandatory	Mandatory	Mandatory
Copies must be limited to individuals authorized to access the data	No Restrictions	Required	Required	Mandatory to individuals permitted under law, regulation, and NAU policies
Data should not be left unattended on a printer or in a public area	No Restrictions	Mandatory	Mandatory	Mandatory
Copies must be labeled "Confidential" or "Sensitive"	No Restrictions	No Restrictions	Required	Required Must follow regulatory and University policies
Electronic copies must use secure copy protocols such as SCP, SSH, SFTP, and SMB 3, and retain all labels	No Restrictions	No Restrictions	Required	Required
USB, CD, DVD, and other removable media containing Highly Sensitive Data must be encrypted and marked/identified	No Restrictions	Encouraged	Required	Required

<b>Data Destruction and Disposal</b> (Hard drives, CDs, DVDs, USB drives, tapes, paper records, etc.) <b>Data Handling Protocol</b>	<b>Level 1 Data</b>	<b>Level 2 Data</b>	<b>Level 3 Data</b>	<b>Level 4 Data</b>
Review the <a href="#">NAU Records Management</a> site for details	Required	Required	Required	Required
Industry standards for secure wiping, degaussing should be followed – deleting or reformatting media is not sufficient	No Restrictions	Required	Required	Required In some cases, the physical media may need to be destroyed or shredded

<b>Electronic Mail Data Handling Protocol</b>	<b>Level 1 Data</b>	<b>Level 2 Data</b>	<b>Level 3 Data</b>	<b>Level 4 Data</b>
Emailing data	No Restrictions	Permitted to send to authorized University Community members and authorized third parties	Mandatory  Contact Information Security Services for guidance	Mandatory  Contact Information Security Services for guidance
Encryption (NIST approved levels) is required when email must be used	No Restrictions	No Restrictions	Required	Required

<b>Network Security Data Handling Protocol</b>	<b>Level 1 Data</b>	<b>Level 2 Data</b>	<b>Level 3 Data</b>	<b>Level 4 Data</b>
May reside on a public network	No Restrictions	Mandatory	Mandatory	Mandatory
Protection with a firewall	Encouraged	Required	Required  The firewall ruleset should follow a default "deny-all" rule for inbound traffic and be reviewed frequently.	Required  The firewall ruleset should follow a default "deny-all" rule for inbound traffic and be reviewed frequently.
IDS/IPS protection	Encouraged	Required	Required	Required
Protection with router ACLs	No Restrictions	Encouraged	Required	Required
Servers hosting the data should be placed on private subnets and not be visible to the entire Internet, or to unprotected subnets such as residence hall or guest wireless networks	No Restrictions	Encouraged	Required	Required
The firewall ruleset should follow a default "deny-all" rule for inbound traffic and be reviewed frequently	No Restrictions	Encouraged	Required annual reviews	Required minimum annual reviews
Logging, monitoring and alerting must be configured and reviewed	No Restrictions	Encouraged	Encouraged	Required

<b>Physical Security Data Handling Protocol</b>	<b>Level 1 Data</b>	<b>Level 2 Data</b>	<b>Level 3 Data</b>	<b>Level 4 Data</b>
System must be password protected when unattended	Required	Required	Required	Required
Hosted in a Secure Data Center	No Restrictions	Encouraged	Required	Required
Physical access must be monitored, logged, and limited to authorized individuals at all times	No Restrictions	Encouraged	Required	Required

<b>Remote Administration Data Handling Protocol</b>	<b>Level 1 Data</b>	<b>Level 2 Data</b>	<b>Level 3 Data</b>	<b>Level 4 Data</b>
Access restricted to local network or NAU Virtual Private Network (VPN)	No Restrictions	Required	Required	Required
Two-Step Verification and authentication	No Restrictions	Encouraged	Required	Required
Some data use agreements may require a secure remote desktop service, "jumpbox" for remote access	No Restrictions	No Restrictions	Encouraged	Required

<b>Storage Data Handling Protocol</b>	<b>Level 1 Data</b>	<b>Level 2 Data</b>	<b>Level 3 Data</b>	<b>Level 4 Data</b>
Storage on a CIO's, or their designee's, approved secure server	Encouraged	Encouraged	Required	Required
Storage in a secure Data Center	Encouraged	Encouraged	Required	Required
Data prohibitions for storing data individual workstation or a mobile device	No Restrictions	Required	Mandatory	Mandatory
Full-disk encryption (FDE)	Encouraged	Required	Required	Required
All storage locations must employ NIST approved encryption levels, anonymization, and/or redaction as required by law or data use agreements	No Restrictions	Required	Required	Required
Encryption of backup media	No Restrictions	Required	Required	Required
Paper/hard copy: do not leave unattended where others may see it; store in a secure and locked location	No Restrictions	No Restrictions	Required	Required
Third party storage and processing may be used if NAU has appropriate contract with vendor	No Restrictions	No Restrictions	Required	Required
USB, CD, DVD, and other removable media containing Highly Sensitive Data must be encrypted and marked/identified	No Restrictions	Encouraged	Required	Required

<b>System Security Data Handling Protocol</b>	<b>Level 1 Data</b>	<b>Level 2 Data</b>	<b>Level 3 Data</b>	<b>Level 4 Data</b>
Must follow University specific and OS-specific best practices for system management and security, including patching/updating, vulnerability scanning, Anti-virus installation	Required	Required	Required	Required
Host-based software firewall	No Restrictions	Required	Required The firewall ruleset should follow a default "deny-all" rule for inbound traffic and be reviewed frequently.	Required The firewall ruleset should follow a default "deny-all" rule for inbound traffic and be reviewed frequently.
Host-based software IDS/IPS	No Restrictions	No Restrictions	Required	Required
Should not be used for web-browsing or email	No Restrictions	No Restrictions	Encouraged	Required
Should not be accessible via public network. Must employ logging, monitoring, and alerting	No Restrictions	No Restrictions	Encouraged	Required

<b>Training Data Handling Protocol</b>	<b>Level 1 Data</b>	<b>Level 2 Data</b>	<b>Level 3 Data</b>	<b>Level 4 Data</b>
General security awareness training	Encouraged	Required	Required	Required
Data security training	No Restrictions	Required	Required	Required
Applicable policy and regulation training	No Restrictions	Required	Required	Required

<b>Transmission Data Handling Protocol</b>	<b>Level 1 Data</b>	<b>Level 2 Data</b>	<b>Level 3 Data</b>	<b>Level 4 Data</b>
NIST approved encryption is required when transmitting via network and secure protocols such as TLS, HTTPS, SFTP, SSH, SMB 3 must be used	No Restrictions	Encouraged	Required Cannot transmit via email unless encrypted and secured with a digital signature	Required Regulated data may be redacted if approved in data use agreement
Where TLS/SSL certificates are used, only secure protocols and cipher suites must be used and the certificate must be signed by a well trusted authority such as Sectigo/InCommon, Let's Encrypt or a centrally managed locally trusted CA. Invalid certs should never be used	Encouraged	Encouraged	Required	Required