

DATA HANDLING PROTOCOLS

In accordance with Northern Arizona University's [Data Classification and Handling](#) policy, the Chief Information Officer ("CIO") and Chief Institutional Data Officer updates and revises as necessary and appropriate 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 2 Internal Data – Low Risk**
- **Level 3 Sensitive Data – High Risk**
- **Level 4 Highly Sensitive Data – Very High Risk**

Further, 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 Institutional Data Officer, or Information Security Services with questions about data classification and handling and the best means of protection.

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 Chief Institutional Data Officer, or Information Security Services with any inquiry or feedback regarding these protocols.

- [Access Controls](#)
- [Backup/Disaster Recovery](#)
- [Copying/Printing](#)
- [Data Destruction and Disposal](#) (Hard drives, CDs, DVDs, USB drives, tapes, paper records, etc.)
- [Electronic Mail](#)
- [Network Security](#)
- [Physical Security](#)
- [Remote Access](#)
- [Storage](#)
- [System Security](#)
- [Training](#)
- [Transmission](#)

In the tables below—

- "No Restrictions" means the data can be publicly disclosed without limitations;
- "Recommended" 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; and
- "Restricted" 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.

Access Controls Data Handling Protocol	Level 1 Data	Level 2 Data	Level 3 Data	Level 4 Data
Open access to public information	No Restrictions	Restricted	Restricted	Restricted
Viewing and modification restricted to authorized individuals	No Restrictions	Restricted	Restricted	Restricted
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	Recommended	Recommended	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

Backup/ Recovery Data Handling Protocol	Level 1 Data	Level 2 Data	Level 3 Data	Level 4 Data
Daily backups to a CIO-approved solution	Required	Required	Required	Required
Encryption of backups	No Restrictions	Recommended	Required	Required
Off-site storage	No Restrictions	Recommended	Required	Required
Backups should be tested periodically	Recommended	Recommended	Required	Required

Copying/Printing Data Handling Protocol	Level 1 Data	Level 2 Data	Level 3 Data	Level 4 Data
Data should only be printed when there is a legitimate need	No Restrictions	Restricted	Restricted	Restricted
Copies must be limited to individuals authorized to access the data	No Restrictions	Required	Required	Restricted 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	Restricted	Restricted	Restricted
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	Recommended	Required	Required

Data Destruction and Disposal (Hard drives, CDs, DVDs, USB drives, tapes, paper records, etc.) Data Handling Protocol	Level 1 Data	Level 2 Data	Level 3 Data	Level 4 Data
Review the NAU Records Management 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

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

Network Security Data Handling Protocol	Level 1 Data	Level 2 Data	Level 3 Data	Level 4 Data
May reside on a public network	No Restrictions	Restricted	Restricted	Restricted
Protection with a firewall is required	Recommended	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 required	Recommended	Required	Required	Required
Protection with router ACLs optional	No Restrictions	Recommended	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	Recommended	Required	Required

The firewall ruleset should follow a default "deny-all" rule for inbound traffic and be reviewed frequently	No Restrictions	Recommended	Required annual reviews	Required minimum annual reviews
Logging, monitoring and alerting must be configured and reviewed	No Restrictions	Recommended	Recommended	Required

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

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

Storage Data Handling Protocol	Level 1 Data	Level 2 Data	Level 3 Data	Level 4 Data
Storage on a CIO approved secure server recommended	Recommended	Recommended	Required	Required
Storage in a secure Data Center	Recommended	Recommended	Required	Required
Storage on an individual workstation or a mobile device	No Restrictions	Recommended If necessary, encryption is required on device.	Restricted If necessary, supervisor approval must be documented	Restricted
Full-disk encryption (FDE) is recommended	Recommended	Recommended	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	Recommended	Required Supervisor approval must be documented	Required
Encryption of backup media is required	No Restrictions	Recommended	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	Recommended	Required	Required

System Security Data Handling Protocol	Level 1 Data	Level 2 Data	Level 3 Data	Level 4 Data
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 required	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 recommended	No Restrictions	No Restrictions	Required	Required
Should not be used for web-browsing or email	No Restrictions	No Restrictions	Recommended	Required
Should not be accessible via public network. Must employ logging, monitoring, and alerting	No Restrictions	No Restrictions	Recommended	Required

Training Data Handling Protocol	Level 1 Data	Level 2 Data	Level 3 Data	Level 4 Data
General security awareness training	Recommended	Required	Required	Required
Data security training required	No Restrictions	Required	Required	Required
Applicable policy and regulation training required.	No Restrictions	Required	Required	Required

Transmission Data Handling Protocol	Level 1 Data	Level 2 Data	Level 3 Data	Level 4 Data
<p>NIST approved encryption is required when transmitting via network and secure protocols such as TLS, HTTPS, SFTP, SSH, SMB 3 must be used</p>	<p>No Restrictions</p>	<p>Recommended</p>	<p>Required Cannot transmit via email unless encrypted and secured with a digital signature</p>	<p>Required Regulated data may be redacted if approved in data use agreement</p>
<p>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 or Let's Encrypt or a centrally managed locally trusted CA. Invalid certs should never be used</p>	<p>Recommended</p>	<p>Recommended</p>	<p>Required</p>	<p>Required</p>