# DATA CLASSIFICATION AND HANDLING

Effective Date: January 31, 2021
Last Revised: TBD

## DATA HANDLING PROTOCOLS

In accordance with Northern Arizona University's Data Classification and Handling policy, the Chief Information Officer ("CIO"), or their designee, 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 CIO's designee, 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 Administration
- Storage
- System Security
- Training
- Transmission

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 parities on a case-by-case basis.

| **Access Controls Data Handling Protocol** | **Level 1 Data** | **Level 2 Data** | **Level 3 Data** | **Level 4 Data** |
|---|---|---|---|---|
| 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~~access~~ are required to be on NAU authorized networks | Required | Required | Required | Required |

| Backup/ Recovery Data Handling Protocol | Level 1 Data | Level 2 Data | Level 3 Data | Level 4 Data |
|---|---|---|---|---|
| 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 |

| Copying/Printing Data Handling Protocol | Level 1 Data | Level 2 Data | Level 3 Data | Level 4 Data |
|---|---|---|---|---|
| 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 |

| **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<br>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 | Mandatory<br><br>Contact Information Security Services for guidance | Mandatory<br><br>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 | Mandatory | Mandatory | Mandatory |
| Protection with a firewall | Encouraged | Required | Required<br><br>The firewall ruleset should follow a default "deny-all" rule for inbound traffic and be reviewed frequently. | Required<br><br>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 |

| **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 | No Restrictions | Encouraged | Required | Required |

| | | | | |
|---|---|---|---|---|
| Physical access must be monitored, logged, and limited to authorized individuals at all times | No Restrictions | Encouraged | Required | Required |

| Remote Administration 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 | Encouraged | Required | Required |
| Some data use agreements may require a secure remote desktop service, "jumpbox" for remote access | No Restrictions | No Restrictions | Encouraged | Required |

| Storage Data Handling Protocol | Level 1 Data | Level 2 Data | Level 3 Data | Level 4 Data |
|---|---|---|---|---|
| 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 ~~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 | Required~~Recommended~~ | Required | Required |
| Encryption of backup media | No Restrictions | Required~~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 | Encouraged | 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 | No Restrictions | Required | Required<br><br>The firewall ruleset should follow a default "deny-all" rule for inbound traffic and be reviewed frequently. | Required<br><br>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 |

| Training<br>Data Handling Protocol | Level 1<br>Data | Level 2<br>Data | Level 3<br>Data | Level 4<br>Data |
|---|---|---|---|---|
| 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 |

| Transmission<br>Data Handling Protocol | Level 1<br>Data | Level 2<br>Data | Level 3<br>Data | Level 4<br>Data |
|---|---|---|---|---|
| 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<br><br>Cannot transmit via email unless encrypted and secured with a digital signature | Required<br><br>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 |