DATA CLASSIFICATION AND HANDLING

Effective Date: January 31, 2021
Last Revised: August 19, 2022

DATA HANDLING PROTOCOLS

In accordance with Northern Arizona University Data Classification and Handling policy, the Chief Information Officer 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 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

dC 89 506.95 Tm0 g0 G[ )]TJETQ0.00000912 0 612 792 reW*n.83 TJ94( )-10(S)4(ec)-3(u)-9(r)-3(i)5(t)-10(y)18( )]TJETQ0.000030080 612 79

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

Electronic Mail Data Handling Protocol	Level 1 Data	Level 2 Data	Level 3 Data	Level 4 Data

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**

Storage Data Handling Protocol	Level 1 Data	Level 2 Data	Level 3 Data	Level 4 Data

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				

Transmission Data Handling Protocol	Level 1 Data	Level 2 Data	Level 3 Data	Level 4 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	Recommended	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 or Let's Encrypt or a centrally managed locally trusted CA. Invalid certs should never be used	Recommended	Recommended	Required	Required