SECURE DATA CENTER PHYSICAL SECURITY

Northern Arizona University owns or controls, and acts as custodian for, a broad array of information, including Highly Sensitive Information protected by law. Maintaining the integrity and availability of this information is an important University function. To this end, Information Security Services deploys a comprehensive framework of *Information Security Standards* of which this document is a part. All members of the University community are required to comply with these requirements. Capitalized terms used herein are defined in the *Information Security* policy or the *Data Classification and Handling* policy. Questions regarding these *Information Security Standards* should be directed to Information Security Services.

This Information Security Standard outlines minimum requirements for protecting Secure Data Centers and other approved IT facilities from physical harm and unauthorized access.

1. Approved Information Technology ("IT") Facilities.

1.1. Approved IT facilities include, but are not limited to, Secure Data Centers, Premises Wire Distribution Closets, and wall-mounted telecommunication cabling racks. A Secure Data Center is a University-managed facility for housing computer, data storage, and/or network equipment that is protected with restricted physical access, environmental controls, power protection, and network firewalls.

1.2. The Chief Information Officer ("CIO") must approve all IT facility locations and must ensure that each IT facility is appropriately kept safe, secure, and protected from physical harm and unauthorized access. Facility management officials must consult with the CIO regarding any plan or action that may impact installed or planned IT facilities or the sensitive resources they contain.

2. Secure Data Center Access Controls.

2.1. Restricted access to Secure Data Centers will be maintained by employing a formal, documented process to authorize entry only by appropriate personnel.

2.2. The Secure Data Center manager will maintain up-to-date lists of all personnel authorized to access Secure Data Centers and will review these lists quarterly to ensure their accuracy and completeness.

2.3. Access privileges for individuals who change roles or depart the University will be revoked with all such changes carefully documented.

2.4. In accordance with federal regulations (NIST 800-53), access to approved IT facilities where classified information is stored must be carefully restricted to only authorized individuals.

3. Access Controls.

3.1. Secure Data Centers must be secured to prevent unauthorized access with physical entry and exit controls deployed that restrict access to only authorized personnel.

3.2. Physical control mechanisms, such as identification badge or card readers, high quality key or combination locks, or biometric scanners, will be deployed as needed to maintain security.

3.3. Visitors to restricted areas are always to be escorted by authorized personnel and must sign-in upon entry and sign-out upon exit. The signing process will record the visitor's name, time, date, reason or purpose for entry, and the escort's name.

4. **Monitoring**.

   4.1. Video monitoring must always be employed to record entry and exit of all individuals.

   4.2. Information Technology Services will audit Secure Data Center visitor logs on a regular schedule and immediately following any instance of a suspected or possible breach event.

   4.3. Information Technology Services will conduct, or cause to be conducted, random testing by "unauthorized individuals" who attempt to access secure facilities as a means of auditing security practices.

5. **Emergency and Climate Controls**.

   5.1. Emergency power sources, such as backup generators, uninterruptible power supplies and redundant cooling systems should be employed in Security Data Centers.

   5.2. Emergency lighting and remote emergency power off ("REPO") must be provided in each Secure Data Center and in other IT facilities as appropriate.

   5.3. Fire protection, suppression, and detection systems that automatically activate and notify emergency responders must be present, active, and regularly tested.

   5.4. Temperature and humidity monitors must be deployed in all Secure Data Centers and server rooms.

   5.5. Water damage prevention controls such as master shutoff valves that are immediately accessible to authorized individuals, must be installed.

   5.6. Inspections will be performed annually to assess all environment controls, with all deficiencies resolved within thirty (30) days.

6. **Deliveries and Removals**.

   6.1. All Secure Data Center deliveries must be pre-authorized and documented. Equipment may only be moved or removed with prior authorization from the Secure Data Center manager.

   6.2. Disposal of equipment must occur in accordance with the University's Data Handling Protocols and all other applicable disposal/destruction requirements. Documentation of all disposal and destruction activities is mandatory and must include date, time, asset inventory number, and all system information, including the data store.

7. **Sensitive Data Breach Response Protocols**.

   7.1. Immediate reporting to Information Security Services of any suspected or actual release or breach of sensitive data, systems, or devices is absolutely mandatory. **Dial 928-523-3335 to make a report**.

   7.2. Upon receiving a report of suspected or actual release or breach of sensitive data, systems, or devices, Information Security Services, in collaboration with appropriate University stakeholders, is responsible for notifying all affected and responsible parties.

   7.3. The CIO will assemble an incident response team to investigate, preserve evidence, mitigate the situation, and analyze and report on the event.

   7.4. In incidences where health or safety may be a concern, the reporting party or Information Security Services will immediately notify the Northern Arizona University Police Department and any external authorities as may be appropriate.