FORT HAYS STATE UNIVERSITY

University Policies
www.fhsu.edu/policies/

POLICY TITLE: Physical Security of Data Center and University Data

---

POLICY PURPOSE: The purpose of this policy is to ensure the physical security of University Data.

BACKGROUND: KITEC Information Technology Policy 7230 instructs state agencies to implement physical access and physical environmental controls.

APPLIES TO: The Data Center, Backup Site, and electronic media containing University Data.

DEFINITIONS:

Data Center: Tomanek Hall Room 111

Backup Site: Sternberg Museum Room 132

KITEC: Kansas Information Technology Executive Council

Electronic Media: Electronic or digital material on which data are or may be recorded, such as magnetic disks or tapes, solid state devices like hard drives and USB flash drives, or optical discs like CDs and DVDs.

System Users: Faculty, staff, students, official university affiliates, and any other individuals who use FHSU computing resources.

University data: Electronic information providing support to and meeting needs of the University community. Data includes, but is not limited to:

- Elements supporting financial management;
- Student records;
- Payroll;
- Personnel records;
- Capital equipment inventory; and,
- Any electronic information:
    - Used for planning, managing, reporting, or auditing a major administrative function;
    - Referenced or used by a Department(s) or College(s) to conduct University business;
    - Included in a University administrative report; or,
    - Used to derive a data element meeting any of the criteria above.

CONTENTS:

Contents

POLICY STATEMENT:

Safeguards for all University Data

Access to the Data Center, Backup Site, and electronic media containing University Data or backups will be restricted to authorized personnel only.

Authorized personnel will ensure appropriate safeguards when electronic media is transported outside of a controlled area, including when media is transported between the Data Center and Backup Site.

Devices containing electronic media, including laptops and USB drives, must be stored securely when unattended. Appropriate secure storage methods include storage in a locked private office, storage in a locked cabinet or closet, or similar. Devices must not be left unattended in an unlocked vehicle or other public location.

Safeguards Specific to the Data Center and Backup Site

The ISO or designee will maintain a list of all authorized personnel with physical access to the Data Center and Backup Site. This list will be reviewed and updated annually, or as user access privileges change.

Authorized users are required to authenticate themselves prior to entry to the Data Center or Backup Site.

All visitors to the Data Center must be escorted by authorized personnel at all times.

All visitor access must be logged.

The Data Center will implement physical environmental controls that mitigate or prevent damage from water, fire, temperature, and humidity.

Sufficient power protection will be available for critical information systems to perform an orderly shutdown.

Procedures and standards for the above statements are listed in the Physical Security of Data Center and University Data Procedure.

EXCLUSIONS OR SPECIAL CIRCUMSTANCES:

Policies:

RELATED DOCUMENTS:	Acceptable Use Policy Endpoint Protection and Configuration Policy Information Security Policy Media Sanitization and Disposal Policy **Forms:** **Other:** Physical Security of Data Center and University Data Procedure
KEYWORDS:	Data center, university data, physical security, environmental security
RESPONSIBLE OFFICE:	Division of Technology Services
RESPONSIBLE UNIVERSITY OFFICIAL:	Director of Technology Services
ORIGINATION DATE:	1/2017
CHANGE HISTORY:	Approved by ELT 7/17/2017