Responsible Office: CITS
Date Established: August 8, 2017
Date Last Revised: August 8, 2017
Date Posted: September 8, 2017

DATA CENTER AND NETWORK PHYSICAL ACCESS POLICY

SUMMARY

The purpose of this policy is to establish the standards by which data centers and Network/telecommunication rooms at Alcorn State University are protected against unapproved physical entry and potentially damaging environmental factors. The Alcorn State University Center for Information Technology Services (CITS) is charged with overall responsibility for properly securing and monitoring these sensitive support areas.

SCOPE

The Alcorn State University IT Physical Access/Environmental Security Policy focuses on CITS Data Centers, Network and Telecommunication Closets.

POLICY STATEMENT

1. Data Centers/Network Closets will be monitored for environmental hazards including heat, water intrusion, fire, and wind / smoke.
2. Security alarm and intrusion prevention systems must be maintained inside all data centers and the facility must be secured outside of normal operating hours.
3. All Data Centers must have security cameras. Occupants of such facilities have no expectation of the right to privacy.
4. Anyone entering a Data Center must be properly documented as being a staff member within CITS, a contractor for CITS, or be accompanied by a member of CITS. Visitors must be properly identified with a current, valid form of identification and must be given a temporary facility badge allowing access to certain areas within the data center.
5. Authorization for access to any facility under this policy must have the appropriate sponsorship of the CIO, Manager of Data Center Services, Manager of Telecommunications or Manager of Network Services. This sponsorship may be revoked at any time and for any reason deemed necessary by the sponsor.
6. Access to any facility under this policy will be to conduct work directly related to the staff or contractor responsibility and in support of the equipment and processes within the facility.
7. Access keys or cards will only be issued to sponsored individuals. All keys and access cards must be documented with the Alcorn State University CITS Department. Access keys or

cards must be returned to the Alcorn State University CITS Department upon termination of employment or termination/completion of a contract.

8. No access keys or cards may be shared between staff or contractors.
9. Loss or theft of access keys or cards must be reported immediately to the CIO or CITS HelpDesk.

PROCEDURE

1. CITS will investigate any incident involving unauthorized access or improper use of any facility under this policy in coordination with law enforcement or appropriate administrative departments.

2. Alcorn State University cooperates fully with federal, state, and local law enforcement authorities in the conduct of criminal investigations. Failure to adhere to the provisions of this policy statement may result in:
    a. Loss of Alcorn State University Information Resources access privileges,
    b. Disciplinary action up to and including termination of employees, contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion, in the case of a student.
    c. Civil or criminal prosecution.

CONTACT INFORMATION

- Contact the CITS department for further information: (601) 877-6182