**POLICY & PROCEDURE DOCUMENT**

NUMBER: 05.5130

UNIT: Information Technology Services

TITLE: Data Center Access

DATE: August 12, 2019

REVISED: N/A

Authorized: AVP for Information Technology Services

## I. Purpose and Scope

WKU Information Technology Services (ITS) Data Centers house equipment and data that are critical to the operation of the University. The purpose of this policy is to reduce risk to the University by restricting physical access to these facilities.

## II. Policy

A. Definitions

1. Authorized-Staff – a University employee who is authorized to enter a WKU ITS Data Center autonomously and unescorted.

2. Authorized-Contractor – a Non-University employee who, through contractual arrangement or approvals, is authorized to access to a WKU ITS Data Center.

3. Authorized-Visitor – a person who may visit a WKU ITS Data Center but is not authorized for unescorted access.

4. Credential – In the context of an Electronic Access Control system a credential may be in the form of, but is not limited to, RFID Cards, RFID Fobs, specialized software on mobile devices, and biometrics. A credential represents the holder of said credential for the use of electronically determining authorization.

5. Electronic Access Control (EAC) – A system comprised of electronic hardware, software, and credentials to grant or deny access to physical spaces. This is in contrast to the use of physical/mechanical keys to provide access to physical spaces.

B. Access to Data Centers

1. Authorization will be granted only if an operational need exists for the access.

2. If the date(s) and time(s) of access for a given Authorized-Staff can be restricted, they will be technologically enforced (i.e. via Electronic Access Control) when possible.

3. Personnel who access a WKU ITS Data Center must have proper authorization on file.

4. If an Authorized-Staff's justification for access is no longer valid (i.e. role/duty change or change in employment status), it must be reported immediately by the affected individual or their supervisor whichever is applicable in the given situation. Authorization will be revoked and access removed.

5. The Authorized-Staff roster will be audited annually, at a minimum.

6. Individuals without proper authorization, but with an operational need to enter a WKU ITS Data Center, must be treated as a visitor.

7. Authorized-Visitors must follow the Visitor Procedures.

8. All Authorized-Contractors will have time-limited access. A defined, last date and time of access is required, which will correspond to the scope of their work. Access will be limited to only the date(s) and time(s) required (i.e. specific start/stop times, day-of-week restrictions, etc.).

9. All access to the Data Centers will be by Electronic Access Control. Physical/Mechanical key access will only be granted to few select employees who would respond in the event of a disaster or other catastrophic failure that may disable the Electronic Access Control system. Physical/Mechanical key holders are to utilize Electronic Access Control for access unless it is non-functional.

**III. Procedure**

A. Access Authorization

1. Authorized-Staff Procedures

    a. Staff Authorization must be granted by the Director covering the Systems/Data Center team or by the senior-most administrator of ITS.

    b. The WKU ITS Systems/Data Center team will be responsible for maintaining authorization records.

2. Contractor Procedures

    a. Contractor authorization may be granted by a member of the ITS Systems/Data Center team.

    b. Whenever viable, it is recommended to utilize visitor procedures for Authorized Contractors.

3. Visitor Procedures

    a. Visitors must be accompanied by an Authorized-Staff member at all times while in a WKU ITS Data Center.

4. Audit Procedures

    a. The WKU Office of IT Security and Identity Management will be responsible for audit procedures.

    b. Regular audit procedures will include a review of access rosters and authorizations as well as spot-checks of Electronic Access Control logs for data center entrances.

**IV. Related Policies**

5.501X Information Security Policy
5.501X Information Security Plan

**V. Reason for Revision**

N/A

This policy was last reviewed on August 12, 2019.