Data Center Access Policy

Policy #:	IT006.1
Policy Type:	University
Responsible Executive:	VP for ISSS
Responsible Office:	OIT
Originally Issued:	April 5, 2023
Latest Revision:	April 5, 2023
Effective Date:	April 5, 2023

I. Policy Statement

The ULM Office of Information Technology (OIT) is charged with the physical security and oversight of critical IT systems.

II. Purpose of Policy

This policy will address the proper handling and review of physical personnel occupancy and access within OIT's primary Data Center located in Walker 1-89. OIT will track and report every person(s) entering and exiting the Data Center.

III. Applicability

This policy applies to all University personnel, contractors, and visitors

IV. Definitions

Data Center – The ULM Data Center is housed in Walker Hall Room 1-89. This facility houses the University's critical applications and data. The network of computing and storage resources enables the delivery of shared applications and data. The key components of the Data Center design include routers, switches, firewalls, storage systems, servers, and application-delivery controllers.

V. Policy Procedure

Access to the Data Center

All doors to the Data Center must remain locked at all times and may only be temporarily opened for periods not to exceed that minimally necessary in order to:

- Allow officially approved and logged entrance and exit of authorized individuals.
- Permit the transfer of supplies/equipment as directly supervised by an OIT employee.
- Prop open a door to the Data Center ONLY if it is necessary to increase airflow into the Data Center in the case of an air conditioning failure. In this case, staff personnel with General Access must be present and limit access to the Data Center.

The Data Center has a primary entrance (front) and rear exit with no windows facing the outside. Each entrance is protected by a minimum of two doors that requires a key and ID badge to gain access. The front entrance has an outside door that can only be accessed with a physical key. The next door to the front entrance requires both a physical key and a simultaneous ID badge swipe to enter the server room. The back entrance requires gaining entrance through 3 doors. The first is a gated door that requires a key or ID Badge to enter, the second door requires a different physical key, and finally the third door can be opened by key or ID badge.

Visitor Logging

The Data Center is a restricted area with a much greater level of control than normal non-public spaces. Only those individuals who are expressly authorized to do so may enter this area. Access privileges will be granted to individuals who have a legitimate business need to be in the Data Center. All third parties and visitors will be required to enter through the primary entrance (front) of the Data Center. All visitors will be recorded entering the Data Center. This will be accomplished with three different methods.

Method 1. All employees that have been granted access to the Data Center will be required to use their physical key and ID badge to gain access to the Data Center. The Genetec system will digitally log employees entering the Data Center using an electronic kiosk.

Method 2. Third parties or visitors who require access to the Data Center will be required to sign in/out of the visitor's log. This will require name, date, time in/out, purpose of visit, and signature of the visitor. Additionally, an approved employee will be required to accompany the visitor into the Data Center until their business is complete. "Piggy backing" with an employee who has access is not permitted. Each visitor is required to sign in/out each time they access the Data Center. The visitor logs will be retained for a minimum of 7 years.

Method 3. All people who enter the server room are also logged through a video surveillance system. The surveillance system monitors the front entrance as well as the Data Center too. All video is retained for approximately one (1) month.

At the end of each month, an employee will be responsible for collecting all visitor logs to be reviewed. This will include converting the physical visitor logs into a digital format as well as obtaining a report from the Genetec system. All visitor logs will be submitted for approval to the Enterprise System & Security Manager and the IT Director for final review. A copy of the report will be stored on a data server at the location specified below.

Visitor Logs Location:
Shared server resource: \\spock.ulm.edu\ucc\Shared\Server Room Logs

VI. Enforcement

Log content is reviewed and a report created monthly. The enforcement is dictated by physical access into the facility by key and electronic ID access. OIT personnel will be responsible for any guest access entrance that was recorded in the log.

VII. Policy Management

The Responsible Executive is the VP for Information Services and Student Success.
The Responsible Office is the Office of Information Technology.
The Responsible Officer is the Director of OIT.

VIII. Exclusions

N/A

IX. Effective Date

This policy is effective upon the date signed by the University President.

X. Adoption

This policy is hereby adopted on this 5th day of April 2023.

Recommended for Approval by:

Dr. Michael A. Camille
VP for Info Services and Student Success

Approved by:

Dr. Ronald L. Berry, President

XI. Appendices, References and Related Materials

N/A

XII. Revision History

Original Adoption Date: April 5, 2023