PURPOSE
To establish the controls and security requirements for gaining physical access to MAIS restricted computing facilities.

SCOPE
This policy is effective for:

- The computer rooms 1103, 1108 and 1118 ASB
- The telecommunications closet, A.K.A. the switch room, (1106 ASB)
- All personnel accessing either the computer room or the switch room

GENERAL
All University information processing and communications areas must be protected by physical controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations.

1. Physical access to restricted facilities shall be restricted to authorized staff. Authorization is granted by the Manager of Operations based on the applicant's eligibility for access described below. The Data Center entrances are monitored by cameras at all times. The activities of all individuals entering and leaving the data center will be recorded.

2. An authorized staff member will always display an identification badge with their picture and name on it. Whenever in a restricted area, all authorized persons must wear an identification badge on their outer garments so that both the picture and information on the badge are clearly visible. The standard for photo badges is the university M-card. If an individual added to the authorized person list does not possess the M-card, an M-card must be created for them.

3. Staff members who have forgotten their identification badge must obtain a temporary badge by providing a driver's license or another piece of picture identification to the Operations shift supervisor. Such a temporary badge is valid for a single day only.

4. Visitors or other third party guests may be granted access to restricted areas by an authorized staff member. While visitors or guests are in the restricted area, they must be escorted at all times. Visitors and guests must sign-in and record:
   - The date and time entering and leaving the restricted area
   - Full name
   - Driver license number or other picture identification
STANDARD PRACTICE GUIDE

- Telephone number
- Purpose for access to the restricted area
- The name of the authorized staff member who granted the access and will remain their escort

5. Field engineers, contractors, and other service personnel performing maintenance work on equipment located within a restricted area may be granted access by Operations shift supervisor. In such a case, it is the discretion of the shift supervisor of Operations whether the engineer, contractor, or service person is required to have a full-time escort or not. The shift supervisor may issue a temporary access badge for up to 1 day. Service personnel must initially sign-in and record:
  - The date and time entering and leaving the restricted area
  - Full name
  - Company name
  - Telephone number
  - Equipment to be serviced
  - Reason for service

6. Authorized staff members must not permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when authorized persons go through these entrances. Authorized staff members must report any violations such as propped doors or unusual requests to the Operator on duty or the Manager of Operations.

7. Authorized staff members that are working in a restricted area are encouraged to report any person not wearing a badge to the operations shift supervisor. The shift supervisor should follow one of the following scenarios:
  - The person is authorized to be in the room but not wearing their badge. If so, they should be asked to wear their badge.
  - The person is an authorized visitor, field engineer, or guest that does not have an escort. If so, the escort should be rejoined with the visitor.
  - The person is unauthorized to be in the area. If so, the person should be asked to leave immediately and escorted to an exit. If the person declines to leave, UM Public Safety should be contacted at 911 and the situation reported.

8. Unauthorized staff members must not attempt to enter restricted computing areas for which they have not received access authorization.

9. Time restrictions that limit a staff member's access to restricted areas may be established by the Manager of Operations. When time restrictions are enforced, the Manager of Operations will ensure that such restrictions do not prohibit the staff member from performing assigned job duties and responsibilities.

10. Under no circumstances will food or drink of any type be allowed in the data center machine room. No hazardous material is allowed in the data center. Cleaning supplies introduced to the room must be approved by the Manager of Operations.

11. All packing material must be removed from computer equipment/components in the specified staging areas before being moved into the Data Center. This includes cardboard, paper wrap, peanuts, plastic, wood and other such material.

12. Exceptions to the policy can be granted by the Director of Infrastructure Operations.
ELIGIBILITY FOR ACCESS

Physical access to restricted areas is based upon the requirements of a person’s role and/or job description and duties requiring any one of the following activities:

1. Servicing of printers such as changing toner, adding paper, and removing printouts.
2. Attending to computer tape drive, CD-ROM drive or other removable media mount and dismount requests.
3. Servicing of other equipment such as telecommunications equipment.
4. Cycle power on equipment.
5. Pressing buttons or toggling switches that are physically located on equipment,
6. Attach or detach hosts to the network.
7. Perform administrative tasks that can only be performed from consoles located within the restricted area.

RESPONSIBILITIES

Manager, Operations

Monitor and report adherence to this policy. Ensure that physical security standards are met. Maintain history of access information to restricted areas. The access information may be made up of, but is not limited to, electronic transaction records created as authorized staff members enter restricted areas and paper sign-in sheets. Maintain the list of authorized employees, review and update list and keep up-to-date information of the employment status of each authorized employee.

Staff Members

Read, understand, and cooperate with the execution of this policy.