EASTERN MICHIGAN UNIVERSITY
DIVISION of INFORMATION TECHNOLOGY

Procedure

Effective Date	Date of Last Revision
April 26, 2010	

Chapter Name	
8.0 Security	
Chapter Number	**Title**
8.5.P.1	**Security Controlled Spaces – DoIT Employee Access**

1.0 Purpose

To ensure a secure data center environment, only staff that require physical access in order to complete his/her specific job duties shall be permitted entry. This procedure will define the process involved to obtain, review and update access to the data center.

2.0 Governing Policy Number/Document Name	Effective Date
8.5 Security Controlled Spaces	

3.0 Procedure

This procedure applies to any EMU/DoIT staff member who may need physical access to the data center. For individual staff members, please contact your Director, Assistant Director or Associate Director to make a request for data center access on your behalf.

Data Center Access Requests and Access Termination Requests:

Access Criteria:

The following criteria shall be used by DoIT administrators to determine whether an employee is provided access to a security controlled space:

1. Staff members that are assigned physical work space in the security controlled space are provided with access to the room(s).
2. Staff members who require physical access for supporting, maintaining, or managing equipment hosted in a security controlled space are provided with access to the appropriate room(s).
3. Senior DoIT Administrators (CIO and Deputy CIO) are provided with access.
4. Staff members or managers assigned to the Disaster Recovery Assessment Team are provided with access to the room(s).
5. Facilities/Maintenance staff may be provided with ID card access, including (but not limited to) electricians and HVAC technicians experienced with working in these spaces.

Director or designee:

Access Requests or access termination requests may be submitted via paper memorandum or via email to Associate Director IT, Enterprise Operations or Director IT, Network and Systems (Operations Management); Requests must include:

1. Staff member's name
2. Staff member E-ID
3. Request to Add / Modify / Remove Access
4. Duration of Access or note as Permanent (for new access requests)
5. Effective Date of the Request

Operations Management or designee:

1. If request is to add access:
   a. Verify access authorization. Authorization requests shall only be accepted from a DoIT Assistant Director, Associate Director, Director, Deputy CIO or CIO.
   b. If request is incomplete, return to requestor to provide all required information.
   c. Add access via the University ID Card System and/or provide staff member with a combination/pass key.
   d. File access request as record of request. Note on printed access request the time and date that the request was completed along with the signature of the person completing the request.

2. If request is to remove access:
   a. Remove ID card access and/or change combination locks (as required).
   b. File access request as record of request. Note on printed access request the time and date that the request was completed along with the signature of the person completing the request.

Routine Access Review:

Current active access shall be reviewed on a monthly basis via report(s) run from ID Card System. Review shall occur during the first full five day work week of each month.

Production Control Staff:

1. Run report to show current active access to:
   a. PRAYH ICT NC E
   b. PRAYH ICT NC W
2. Review the report and highlight any discrepancies.
3. Sign and date the report to denote date and who reviewed the report for discrepancies.
4. Deliver signed report (with or without highlighted discrepancies) to Operations Management.
5. Operations Management will discuss/review any discrepancies with appropriate Director (or designee) and make needed corrections.
6. Operations Management will sign/date the report to denote when it was reviewed and who reviewed the report.
7. After all discrepancies are resolved, report should be filed and kept for not less than 12 months and a copy provided IT Security for review.

4.0 Responsibility for Implementation

DoIT Operations Management is responsible for overall implementation, administration and interpretation of this procedure.

Production Control is responsible for the implementation and maintenance of access review.

The DoIT Director(s) or designee is responsible for requesting addition/removal of access.

5.0 Definitions

Term	Definition
Operations Management	Either or the combination of the Associate Director IT, Enterprise Operations and/or Director IT, Network and Systems Services

6.0 Revision History

Description	Approval Date
Original	April 23, 2010