EASTERN MICHIGAN UNIVERSITY
DIVISION of INFORMATION TECHNOLOGY

Procedure

Effective Date	Date of Last Revision
July 15, 2013	July 15, 2013

Chapter Name	
Security	
Chapter Number	**Title**
8.15.P.2	**Access Control – DoIT Systems Privileged Access Account Termination**

1.0 Purpose

The purpose of this document is to outline the procedure for requesting termination of elevated privileges granted to Division of Information Technology infrastructure systems.

2.0 Governing Policy Number/Document Name	Effective Date
8.15 Access Control	July 15, 2013

3.0 Procedure

DoIT Associate Director, Director, Deputy CIO or CIO (Requester):

1) E-Mail the access termination request to the DoIT Access Administrator via e-mail at it_security@emich.edu with all of the following required information:
   a) Date and time access is to be disabled (if not immediate).
   b) Name of employee whose access will be terminated.
   c) E-ID.
   d) My.emich ID.
   e) System (or list of systems) for which access termination is required. (If all access should be removed, such as in the case of involuntary termination, please include statement to "REMOVE ALL ACCESS".)

DoIT Access Administrator (or designated on-call security staff member):

2) Review the request and determine what systems require privilege removal and/or account lock/termination.
3) If request specifies "REMOVE ALL ACCESS", search the IT_SECURITY e-mail account's "Access Requests" folder and sub-folders for specified EID, My.emich ID and last name.
4) From archived Access Requests, compile list of all privileged access.
5) E-mail termination order to all relevant network, database, application and/or system administrators directing that privileged access be removed and affected accounts be LOCKED/TERMINATED.

Network, Database, System or Application Administrator:

6) Remove elevated privileges and/or lock/terminate accounts as directed.
7) E-Mail the DoIT Access Administrator to inform him/her the account lock/termination process is complete.

DoIT Access Administrator (or designated on-call security staff member):

8) E-Mail the requester to inform him/her the account lock/termination process is complete.

4.0 Responsibility for Implementation

The Director of Network and System Services is responsible for the implementation of this procedure.

5.0 Definitions

Term	Definition
DoIT Access Administrator	The IT administrator assigned to manage IT Staff access to systems. The Access Administrator is typically the Director of Network and Systems, but the role can be assigned to other managers at the discretion of the Chief Information Officer.
Privileged Access	Elevated permission to access files, install and run programs, and change configuration settings for systems and services.
Requester	The IT Director, Deputy CIO, or CIO submitting the Access request.
Systems Infrastructure	Servers, business applications, databases, web services, and network appliances.

6.0 Revision History

Description	Approval Date
Initial Draft - Jenkins	Sept. 20, 2011
Approved by CIO	July 15, 2013