

 <b>EASTERN</b> <b>MICHIGAN UNIVERSITY</b> <small>DIVISION of INFORMATION TECHNOLOGY</small>	<b>Procedure</b>	
	<b>Effective Date</b>	<b>Date of Last Revision</b>
	July 15, 2013	July 15, 2013

<b>Chapter Name</b>	
Security	
<b>Chapter Number</b>	<b>Title</b>
<b>8.15.P.1</b>	<b>Access Control – DoIT Systems Privileged Access Request</b>

**1.0 Purpose**

The purpose of this document is to outline the procedure for requesting, approving and granting elevated privileges to Division of Information Technology systems infrastructure.

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

**3.0 Procedure**

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

- 1) E-Mail the access request to the DoIT Technical Security e-mail address at: **IT\_Security@emich.edu** with all of the following required information:
  - a) Name of person to be granted access (Grantee)
  - b) E-ID
  - c) My.emich ID
  - d) System for which access is requested
  - e) Description of access required
  - f) Business justification for the access request.
  - g) Date and time access is to be added (Optional, only required for non-immediate requests)
  - h) Duration of access (or permanent) *Note that permanent requests are subject to annual review.*

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

- 2) Review the request.
- 3) The access administrator may deny requests that are inconsistent with best practice, inadequately justified or otherwise deemed inappropriate by the administrator. (Denials may be appealed to the next higher level of IT Management.)
- 4) Once approved, e-mail the request to the appropriate System or Application administrator and direct that the access be granted.
- 5) If denied, e-mail reason for denial to requester.
- 6) File the request in the appropriate subfolder under the “Access Requests” folder of the IT\_SECURITY e-mail account.

**System or Application Administrator:**

- 7) Configure the requested security access.
- 8) E-Mail the Grantee with any pertinent information and to notify them that the access has been configured.

- 9) E-Mail the DoIT Access Administrator and the Requester to inform them the access 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
<b>DoIT Access Administrator</b>	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.
<b>Grantee</b>	The IT Staff member for whom access is being requested by way of this procedure.
<b>Privileged Access</b>	Elevated permission to access files, install and run programs, and change configuration settings for systems and services.
<b>Requester</b>	The IT Director, Deputy CIO, or CIO submitting the Access request.
<b>Systems Infrastructure</b>	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