

 <b>EASTERN</b> <b>MICHIGAN UNIVERSITY</b> DIVISION of INFORMATION TECHNOLOGY	<b>IT Policy 4.8</b>	
	<b>Effective Date</b>	<b>Date of Last Revision</b>
	September 30, 2008	September 26, 2008

<b>Chapter Name</b>	
4.0 Information Management	
<b>Chapter Number</b>	<b>Title</b>
4.8	EMU Systems Accounts

### 1.0 Purpose

The purpose of this policy is to ensure that Eastern Michigan University (EMU) employees, students, alumni, donors, and EMU affiliates are granted appropriate access to EMU’s production environment and network in order to perform their job responsibilities. Timely account maintenance which reflects the current role(s) held by an EMU account holder, including, but not limited to, termination of access improves the security posture of the university and reduces the risk of exposure of confidential information.

### 2.0 Scope

The scope includes all EMU faculty/staff/students/guests and EMU affiliates that use and maintain an account issued by the Division of Information Technology. An account is necessary for accessing EMU production systems and networks, including but not limited to: email, Banner, NT domains, and shared directories. The scope of this policy is not meant to include system-level administrative accounts internal to the Division of IT.

### 3.0 Policy

Access to computer applications is generally performed through an individual account. EMU computer account permission and the access granted to the account holder are based on the security principles of “**least-required-privilege**” and “**need-to-know**”. The least-privilege principle limits access to the least amount required to perform the job functions. The principle of need-to-know limits access to only that information that is required to perform job responsibilities. With the implementation of both principles, access to EMU data is strictly controlled.

The Division of Information Technology maintains computer account(s) for EMU employees, students, alumni, donors, and EMU affiliates to reflect the appropriate access required to perform the responsibilities associated with the status of their relationship to the university. EMU will strive to implement technology best practices while meeting federal/state/audit requirements for access control and maintenance of computer accounts. These accounts include but are not limited to access to the Enterprise Resource and Planning (ERP) system, EMU provided email, shared storage, and other production applications and systems.

- Accounts will be created based on the relationship with EMU. Employee access will be assigned according to the position being held.
- Escalation of privileges must be requested and approved by the Division of Information Technology.
- Accounts will be maintained as changes in the relationship with EMU occur. These changes may affect the features, functions and data the account holder will have access to.

- Account access will be removed based on type of service being granted and specific conditions or specific duration. Refer to [Attachment A](#).
- Accounts will be removed from the appropriate systems immediately after the conditions in [Attachment A](#) are reached.
- Once accounts are removed from the system, the content will not be restored.

**Controls/Auditing:**

With respect to any account providing access to DoIT-managed central services, the IT Security Office is responsible for access control. Internal system-level accounts or additional restrictive security controls may rest under the control of the respective DoIT department. The IT Security Office may audit through log management any EMU account maintained by DoIT.

**4.0 Responsibility for Implementation**

All account holders are responsible for using the account in accordance with EMU and DoIT policies and procedures.

The Director of IT Security is responsible for implementation of this policy.

**5.0 Enforcement**

Any user found to have violated this policy may be subject to loss of certain privileges or services, and other disciplinary actions or legal sanctions, civil and criminal.

**6.0 Definitions**

<u>Term</u>	<u>Definition</u>
-------------	-------------------

<b>EMU Affiliates</b>	<p>Affiliated third parties are persons or entities that maintain a relationship with the University for (without limiting possible relationships), research, education, military training, service, fund raising, athletic support, or other activities or interests that the University specially recognizes and supports as desirable in carrying out its educational mission, but are not students, employees, or faculty members.</p> <p>Examples of affiliated third parties include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• The Eastern Michigan University Foundation</li> <li>• Military Science and Reserve Officers Training Corps</li> <li>• Emeritus Faculty and Spouses</li> <li>• Emeritus Staff</li> <li>• Grant employees</li> <li>• Temporary employees from an outside agency participating in a University class or project but otherwise not affiliated.</li> <li>• Persons who an authorized WebCaucus organizer desires to be given temporary access to the WebCaucus conferencing system only, for purposes consistent with the University mission.</li> </ul>
<b>Production Environment</b>	<p>Any machine used to store or transfer data between two machines where both machines meet the requirements below:</p> <p>1) are part of the Eastern Michigan University (EMU) Enterprise</p>

<b>Production Environment continued . . .</b>	<p>Resource and Planning System (ERP), or  2) system(s) approved for purchase by the Enterprise Resource and Planning System Tactical Committee (ERP-TAC), or  3) system(s) whose contract is signed by the CIO, or  4) any hardware/software where memorandums of understanding (MOU) agreements are present between DoIT and a department/division, making a machine part of the EMU production environment.</p> <p>Exceptions to the above definition are: applications used for academic classroom projects; systems purchased for DoIT internal use; and duplicate production environments used for testing and training purposes only.</p>
<b>Account Holder</b>	Individual assigned an EMU account by the Division of Information Technology used to access one or more computer systems. When an account has been assigned collectively to a group of individuals or an organization, one individual shall be designated as the Account Holder.
<b>Computer Accounts</b>	A computer account provides access to EMU services and is associated specific rights or privileges for a specific service or computer application.

<b>7.0 Revision History</b>			
<u>Creator</u>	<u>Description</u>	<u>Submission Date</u>	<u>Approval Date</u>
Dorendorf	Initial Draft	August 4, 2008	
Dorendorf	Transfer to IT Policy	August 8, 2008	
IT Policy Committee	Reviewed and approved 08-26-2008; notes sent to email committee 08-27-2008	08-27-2008	
A. Barr	Footer corrected;	09-03-2008	
A. Barr	Final editing	09-08-2008	
Dorendorf	Removed Tracking	September 26, 2008	
Connie Schaffer, Interim CIO	Reviewed and Approved	September 26, 2008	