

 EASTERN MICHIGAN UNIVERSITY <small>DIVISION of INFORMATION TECHNOLOGY</small>	Policy	
	Effective Date	Date of Last Revision
	October 18, 2014	October 16, 2014

Chapter Name	
Security	
Chapter Number	Title
8.1	Passwords for DoIT Systems

1.0 Purpose

Strong passwords are necessary to insure integrity and confidentiality of data and security of information systems. The purpose of this policy is to authorize and direct the establishment of a standard for creation of strong passwords, the protection of those passwords, and the frequency of password change.

2.0 Scope

All members of the Eastern Michigan University community.

3.0 Policy

For all EMU user accounts and systems a password sufficiently complex to prevent unauthorized access is required. The rules for password complexity are established in the standard hereunder.

Different levels of password security, if appropriate, may be created for users and accounts with differing levels of access and authorization, as detailed in the standards, guidelines and procedures derived from this policy.

4.0 Responsibility for Implementation

The director in charge of IT Security is responsible for the implementation of the policy.

5.0 Enforcement

Any employee found to violate federal or State of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under University policy. Any student found to violate federal or State of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under EMU's Student Code of Conduct. Any suspected violation of state or federal laws will be reported to the appropriate legal authority for investigation.

The University reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending computer system from the campus network, terminating a running job on a computer system, or taking other action.

6.0 Definitions	
Term	Definition

7.0 Revision History	
Description	Approval Date
Initial Draft (S. Edwards, A. Edwards, J. Pringle)	September 5, 2014
Policy committee 1 st approval	September 18, 2014
Policy committee 2 nd approval	October 16, 2014
CIO approval	October 18, 2014