EASTERN MICHIGAN UNIVERSITY
DIVISION of INFORMATION TECHNOLOGY

Policy

Effective Date	Date of Last Revision
November 14, 2012	November 14, 2012

Chapter Name	
8.0 Security	
Chapter Number	**Title**
8.8	Vulnerability Scanning and Reporting

1.0 Purpose

The purpose of this policy is to authorize the appropriate use of vulnerability scanning tools necessary to identify and mitigate computer system vulnerabilities.

2.0 Scope

The scope of this policy includes all personnel who are responsible for or who use Eastern Michigan University computer systems as well as all computing devices that are or will be connected to an EMU network. To the extent required and possible to protect sensitive university data, vendors and vendor systems are subject to this policy.

3.0 Policy

All computing devices connected to the Eastern Michigan University network (wired or wireless) are subject to routine vulnerability scanning and reporting. Vulnerability scanning can only be authorized by the Division of Information Technology and only as required to complete assigned duties.

Vulnerabilities identified via scanning shall be reported to the appropriate system administrator for review and resolution. Administrators managing systems containing critical (high-risk) vulnerabilities are required to mitigate those vulnerabilities as quickly as possible.

The Division of Information Technology may remove (or logically isolate) a server or system from the University network if the risk is deemed too high to leave the system available or if the risk is not mitigated in a timely fashion.

4.0 Responsibility for Implementation

The Chief Information Officer and/or the IT Director responsible for Information Security are responsible for implementation and maintenance of this 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**
Vulnerability	A bug or defect in software that renders that software subject to compromise or other unintended or abusive use. Vulnerabilities may be found in the operating system, applications, or other software exposed via a network.
Vulnerability Scanning	A method of comparing the software installed on a server or system to a list of vulnerable software and reporting software that contains vulnerabilities.
Computing Device	Any electronic device connected to the campus wired or wireless network, including but not limited to, desktop computers, laptop computers, tablet computers, and servers.

7.0 Revision History	
Description	**Approval Date**
Original	