EASTERN MICHIGAN UNIVERSITY
DIVISION of INFORMATION TECHNOLOGY

Procedure

Effective Date	Date of Last Revision
January 13, 2014	January 13, 2014

Chapter Name	
Security	
Chapter Number	**Title**
8.15.P.3	**Identification of Anomalous Login Activity**

1.0 Purpose

To outline how anomalous login activity is identified and the threshold that will be used for any IT response or investigatory follow up.

2.0 Governing Policy

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

3.0 Procedure

DoIT System Administrators

1. DoIT System Administrators receive a daily report of anomalous login activity titled "Failed Login Report". The report is automatically generated and delivered to DoIT system administrators.
2. System Administators shall review the report for the systems for which they are responsible.
3. System Administrators shall lock accounts or otherwise respond for accounts that are under attack.

Banner Account Access

1. After five failed login attempts, the Banner system automatically locks the account for 5 minutes.
2. Banner security team shall review excessive failed Banner logins and respond as required if an account is deemed under attack or at high risk.

Log Correlation/SIEM

1. Logs from all systems are delivered to the qRadar log SIEM.
2. The SIEM system classifies and looks for the following anomalous login activity:
    a. Login successful after scan attempt
    b. Login failures to disabled accounts
    c. Login failures to expired accounts
    d. Login failure across multiple hosts/systems
    e. Login failures followed by success
    f. Repeated login failures to a single host.
3. The SIEM system reports correlated results that exceed thresholds defined within that system on the Dashboard of the system to the Security team.
4. The Security team shall review such reports and take appropriate action to resolve any ongoing threats.

Should any of these items result in data that suggests a security incident has occurred, the details shall be reported per the Incident Response procedure.

4.0 Responsibility for Implementation

The director in change of IT security is responsible for the implementation of this procedure.

5.0 Definitions	
Term	**Definition**
Anomolous Login Activity	Any of the following: • Login successful after scan attempt • Login failures to disabled accounts • Login failures to expired accounts • Login failure across multiple hosts/systems • Login failures followed by success • Repeated login failures to a single host

6.0 Revision History	
Description	**Approval Date**
Jenkins – Initial Draft	November 4, 2013
Policy Committee	January 9, 2014
Approved by CIO	January 13, 2014