EASTERN MICHIGAN UNIVERSITY
DIVISION of INFORMATION TECHNOLOGY

# Procedure

| Effective Date | Date of Last Revision |
|---|---|
| 10/28/2013 | 12/19/13 |

| Chapter Name | |
|---|---|
| **Security** | |
| **Chapter Number** | **Title** |
| **8.6.P.1** | **Incident Logging Procedure** |

## 1.0 Purpose

To establish a procedure for tracking IT security incidents as they come in.

| 2.0 Governing Policy<br>Number/Document Name | Effective Date |
|---|---|
| 8.6 Information Systems Security Incident Response | 01/12/2010 |
| | |
| | |

## 3.0 Procedure

This procedure defines how security incidents are logged.

1. A security incident is received by an IT Security Team Member.
2. A log entry is made in a shared Google Doc titled "Incident Log" shared by the Security and Identity Team and the Director responsible for Security.
    a. The log entry assigns an incident number of the format YYYY-MM-DD-## where ## is 01 for the first reported incident on that date and 02 for the second and so on.
    b. The security team member assigned to lead the incident response.
    c. A brief (non-confidential) description of the incident report. Confidential details should only be included in the incident report stored separately.
3. Cateogorization of the incident is handled on a per-incident basis and not included in the log.
4. After the incident number is assigned, all e-mail communications should be tagged using the incident number by including the incident number in the subject line or body of each relevant message.

## 4.0 Responsibility for Implementation

The Director responsible for IT Security is responsible for implementing this procedure.

| 5.0 Definitions<br>Term | Definition |
|---|---|
| | |
| | |
| | |

| 6.0 Revision History<br>Description | Approval Date |
|---|---|
| Jenkins – Initial Draft | 10/28/2013 |
| IT Policy Committee | 12/19/2013 |
| Approved by CIO | 12/19/13 |