**Name of Policy:** Computer incident response.

**Policy Number:** 3364-65-16

**Approving Officer:** Vice President of Information Technology

**Responsible Agent:** Vice President of Information Technology

**Scope:** all University campuses – see paragraph (C)

<table>
<thead>
<tr>
<th></th>
<th>New policy proposal</th>
<th>Minor/technical revision of existing policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>□</td>
<td>Major revision of existing policy</td>
<td>Reaffirmation of existing policy</td>
</tr>
</tbody>
</table>

**Original Effective date:** May 4, 2011

---

(A) Policy statement

Information technology is an integral part of how the university conducts business and maintains information. The university must be prepared to evaluate adverse events effectively and to respond appropriately when incidents are identified. Preparation and planning for an incident, and ensuring that the right resources are available, are critical to the university’s ability to detect, respond and recover from an information technology security incident.

(B) Purpose

This policy identifies security response requirements for identified computer security incidents.

(C) Scope

The scope of this information technology policy includes university computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the university who use and administer such systems.

(D) Requirements

The university will maintain an information technology security incident response capability based on a periodic risk assessment of data, processes, systems, and networks in accordance with The University of Toledo “Information Security Framework.” This capability will provide the ability to determine if an adverse event has become a security incident and, then, how that incident is to be handled. The university’s incident response capability shall include, but not limited to, the following:

1. Incident Response Team. The university incident response team consists of:
   (i) IT Security Office
   (ii) Compliance Officer *
   (iii) Legal Office
   (iv) UT Police Department (as required)
* The Compliance Officer provides coordinating functions throughout the incident response process. This coordination is intended to enable the sharing of information and the prevention of cross-purpose actions.

(2) Incident Response Plan. The Information Technology Department will develop and regularly maintain an incident response plan to evaluate and determine if an adverse event has become an incident. The plan shall also detail the incident response team’s actions in response to an identified security incident.

(E) Incident Reporting

Potential computer security incidents should be reported through any of the Incident Response Team organizations identified in paragraph (D)(1) as appropriate. Following the initial report the organization that receives notification of a potential incident will notify the IT Security Office.

(F) Definitions

(1) Adverse Event. Any observable occurrence with a negative consequence or impact on a system or network. Examples of adverse events include system crashes, network packet floods, unauthorized use of system privileges, defacement of a Web page, execution of malicious code that destroys data, physical security, data or access compromised by accident, and lost or stolen computers.

(2) Incident. A reported adverse event or group of adverse events. An incident may also be an identified violation or imminent threat of violation of information technology security policies, or a threat to the security of system assets. Some examples of possible information technology security incidents are:

(a) Loss of confidentiality of information  
(b) Compromise of integrity of information  
(c) Loss of system availability  
(d) Denial of service  
(e) Misuse of service, systems or information  
(f) Damage to systems from malicious code attacks, such as viruses, trojan horses or logic bombs

(3) Incident Response. A structured and organized response to any information technology security adverse event or incident that threatens an organization’s system assets, including systems, networks and telecommunications systems.
(4) Incident Response Team. A group of professionals within an organization trained and chartered to respond to identified information technology security incidents. The incident response team has both an investigative and problem-solving component and should include management personnel with the authority to act, technical resources with the knowledge and expertise to rapidly diagnose and resolve problems, and communication personnel to keep appropriate individuals and organizations properly informed and develop public image strategies as necessary.

Approved by:

/s/ G. Ovwigho
Vice President of Information Technology

May 5, 2011
Date

Policies Superseded by This Policy:
None

Initial effective date: May 4, 2011
Review/Revision Date: May 4, 2014

Review/Revision Completed by:
Vice President of Information Technology