University of Oklahoma
Information Technology Policies
Subject: Incident Response

I. Purpose
The purpose of this policy is to provide the basis of appropriate reporting of incidents that threaten the confidentiality, integrity, and availability of university information assets, information systems, and the networks that deliver the information. This policy underlies the establishment and ongoing deployment of trained computer security incident response teams, formed with the purpose of managing computer security related incidents at the University of Oklahoma. This effort is being taken to improve the response time for resolving incidents, provide consistent response, and improve incident reporting.

The University of Oklahoma’s computing resources are critical to our mission and should be used appropriately. In order to better protect campus users, computing resources, and sensitive data, all incidents should be reported and investigated.

The IT Security office will respond, investigate, and recover computer security incidents within the framework of the University of Oklahoma Computer Incident Response Plan and the Data Classification Policy. The plan is designed to provide effective coordination between university officials during the incident response process.

II. Scope
This policy applies to users of university owned computing devices and/or users who are connected to the OU network.

III. Policy
The Office of the Vice President for Information Technology is responsible for investigating all Computer Security Incidents (see Definitions below). In order to properly classify and investigate an incident, any records or data that are related to an incident and are under the authority of, or coming in the custody, control or possession of the university, must be made available to the Vice President of Information Technology or designee upon request.

Users must report all computer security incidents promptly to the IT Security Office. Reported incidents will be classified and handled according to the procedures set forth in the University of Oklahoma Computer Incident Response Plan.

IV. Definitions

Computer Security Incident
An anomalous event which results in a loss of confidentiality, disruption of data or system integrity, or disruption or denial of availability of a computer device or network. An incident can be thought of as a violation or imminent threat of violation of IT Security polices or standard security practices.

Examples include, but are not limited to:
- Mishandling or breach of Category II or Category III data (See Data Classification Policy)
- Unauthorized use of computing resources by third party
- Inappropriate usage of computing resource by authorized users (See Acceptable Use Policy)
- Denial of Service attack that renders a computer resource unusable
- Virus, Trojan Horse, or other malware that causes a system disruption and/or data breach

OU Network
Any equipment, owned or controlled by the University of Oklahoma, involved in the processing or forwarding of electronic information. These systems include network devices such as routers, switches, and firewalls.

Computing Device
Any device involved in the processing, storage, or forwarding of electronic information. These devices include, but are not limited to, laptop computers, desktop computers, personal digital assistants, smartphones, and servers.

### IV. Contacts

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Telephone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Contact for Questions</td>
<td>IT Help Desk</td>
<td>405-325-4357</td>
<td><a href="mailto:needhelp@ou.edu">needhelp@ou.edu</a></td>
</tr>
<tr>
<td>Report an Incident</td>
<td>IT Security Office</td>
<td>405-325-7258</td>
<td><a href="mailto:security@ou.edu">security@ou.edu</a></td>
</tr>
<tr>
<td>Legal Issues</td>
<td>Office of Legal Counsel</td>
<td>405-325-4124</td>
<td>none</td>
</tr>
<tr>
<td>Employee Issues</td>
<td>Human Resources</td>
<td>405-325-0776</td>
<td><a href="mailto:ohr@ou.edu">ohr@ou.edu</a></td>
</tr>
<tr>
<td>Threats or Harassment</td>
<td>OUPD</td>
<td>405-325-2864</td>
<td></td>
</tr>
</tbody>
</table>