The purpose of an Information Technology Standard is to specify requirements for compliance with Old Dominion University Information Technology policies, other University policies, as well as applicable laws and regulations. Standards may include business principles, best practices, technical standards, migration and implementation strategies, that direct the design, deployment and management of information technology.

A. PURPOSE

The purpose of this standard is to identify the responsibilities for security monitoring and logging of IT system activity.

B. DEFINITIONS

Information Security Office is the unit within the Office of Computing and Communications Services responsible for overseeing efforts to protect ODU’s computing and information assets and to assist in compliance efforts with information-related laws, regulations, and policies.

Information Security Officer (ISO) is responsible person for developing, reviewing, evaluating, and managing the University’s Information Security Program.

Logging is an essential information security control that is used to identify, respond, and prevent operational problems, security incidents, policy violations, fraudulent activity; optimize system and application performance; assist in business recovery activities; and, in many cases, comply with federal, state, and local laws and regulations.

System Owner is the manager responsible for operation and maintenance of a University IT system.

C. STANDARDS STATEMENT

General Logging Activity
Logging is to be enabled on all IT systems. Logging includes maintaining log detail, log review, log integrity, data classification and log retention.
Employees or other designated individuals with responsibility for logging have some flexibility in determining the detail contained in logs within their areas of responsibility. The detail of information contained in a log depends on the risks to the relevant IT resource and underlying data. However, all system logs must contain a time-stamp associated to the logged event synchronized to the University’s Network Policy Server (NTP.)

All system logs should be devoid of any unencrypted sensitive data, passwords, financial data or personally identifiable information.

**Prohibited Logging**
The use of keystroke logging, except when required for security investigations and approved in writing by the University President, is prohibited.

**Responsibilities**
Designated employees are responsible for the development and implementation of logging capabilities and the creation and maintenance of detailed procedures for reviewing and administering the logs.

Information Security Officer is responsible for Intrusion Detection System (IDS) and In-Plane Switching (IPS) and event correlation logging.

The Director of IT Infrastructure of is responsible for server logging, desktop logging, and network device logging.

The Director of Business Intelligence and Data Services is responsible for database logging.

The System Owners are responsible for application logging.

Information Security Office staff is responsible for monitoring security event logs, correlating information with other automated tools, identifying suspicious activities, and providing alert notifications.

Data Center Operations staff is responsible for monitoring the production computing environment and providing alert notifications.

The Database Administration staff is responsible for monitoring the availability and performance of the databases and for providing corrective actions and/or alert notifications.

**Compliance**
Centralized and departmental IT units and custodians are responsible for ensuring appropriate compliance with this standard for IT resources within their areas of responsibility and are responsible for documenting appropriate compliance.

Documentation should include the type of logging taking place, data classification of the logs, retention periods for the relevant logs, and frequency of log review.
D. PROCEDURES, GUIDELINES & OTHER RELATED INFORMATION

University Policy 3501 IT Access Control Security Policy
University Policy 3505 Security Policy
Information Security Program
Internal Procedures

D. HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Responsible Party</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2006</td>
<td>CIO/ITAC</td>
<td>Created</td>
</tr>
<tr>
<td>October 2007</td>
<td>CIO/ITAC</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2008</td>
<td>CIO/ITAC</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2009</td>
<td>CIO/ITAC</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2010</td>
<td>CIO/ITAC</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2011</td>
<td>CIO/ITAC</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>September 2012</td>
<td>CIO/ITAC</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>January 2012</td>
<td>IT Policy Office</td>
<td>Added time stamp and sensitive data requirement.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added compliance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Revised employee titles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added definitions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Numbering revised.</td>
</tr>
</tbody>
</table>