**Office of Computing and Communications Services**

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.

<table>
<thead>
<tr>
<th>Information Technology Standard:</th>
<th>Server Management Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference Number:</td>
<td>06.5.0</td>
</tr>
<tr>
<td>Date of Current Revision or Creation:</td>
<td>March 20, 2013</td>
</tr>
</tbody>
</table>

**A. PURPOSE**

The purpose of this standard is to define the system inventory requirements used by Old Dominion University.

**B. DEFINITIONS**

**Change Management System** is a process and set of tools by which changes to IT systems are managed, coordinated, approved, communicated and actions logged.

**Hardening Guide** is a document with detailed procedures for server security. Due to the nature of the sensitive material, access is restricted.

**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.

**Server** is a computer system that provides services to other computer systems over a network. Virtual servers are considered servers under the Server Management standard.

**C. STANDARDS STATEMENT**

**System Administration**

System Administrators must process fundamental knowledge and/or experience of the principles, practices, and procedures of the systems and platforms they support. Industry or vendor certifications are recommended. System administrators apply knowledge to ensure that information security risks are managed effectively. System administrators should complete the First Responder course (or equivalent
training) for the appropriate platform. For business continuity, at least two people should monitor vendor communication and other notification sources for relevant system information.

**Documentation**

System configuration documentation is a requirement for all centralized systems. Systems must be operated with the documented configuration and in a manner that provides the best operational performance while applying the greatest information security. Documentation should be current, maintained in a central location and accessible to staff. The level of documentation should be sufficient to:

- Prevent a dependency on a single key staff member
- Provide serial numbers or license keys needed for installation and vendor support
- Test procedures to minimize downtime when changes occur
- Transmit knowledge to others
- Provide the most current documentation

System audit logs are configured and their operation verified immediately on initial system setup. Operational audit logs are maintained on a best effort basis equivalent to 120 days. Logs are reviewed by staff and discrepancies are investigated and resolved as necessary. Systems are configured to generate and centrally store all relevant logs off system. Wherever it is possible, controls and activity auditing should be implemented over the use of utility programs that may provide users the ability to override existing system and application controls.

**Scheduling Systems Operations**

Systems operations and maintenance schedules are planned, authorized, and documented through the Change Management System. System changes should occur within the established standard maintenance window. Changes to operations for mission critical systems are tested in a test environment and approved prior to implementing in production.

**Data and Directory Structures**

The layout and utilization of data directories and structures is coordinated by IT personnel. This information should be outlined in the system configuration documentation previously noted. Users must adhere to the established structure outlines at all times. During system configuration and as needed thereafter, access restrictions to directories are applied as necessary to restrict unauthorized access. Specific types of auditing may be required based on the type of information on the file system.

**Access Control**

Access to information and documents is carefully controlled to ensure that only authorized personnel have access to sensitive information. File system permissions are layered with network access permissions so security can be applied to the file system first and the share second. Network access permissions are applied to prevent non-authenticated users from being able to retrieve directory and file information. All systems should have a minimum of two user accounts that are capable of administering the system.

**Restarting or Recovering the System**

System owners must ensure that adequate back up and system recovery guidelines exist prior to placing a system into production. System administrators are responsible for implementing the direction set by system owners within time and budget.
Operating system changes (such as service packs, updates, fixes, patches or upgrades) are tested for compatibility and released based on a quarterly schedule determined to be the least disruptive and most effective for the environment. All changes will be coordinated with the System Owners. All servers are required to be configured to utilize centrally managed automatic update services. Application changes (such as updates, fixes, patches or upgrades) are tested for compatibility and deployed based on operational requirements of the System Owner. Vendor recommended updates to software undergo a risk-benefit analysis and are carefully scheduled.

Patches and updates are obtained only from reputable or confirmed sources. Major updates to centralized and/or mission critical systems will undertake a formal project plan and cycle through the Production Change System.

**Hardening Operating Systems**

Server operating systems are configured to operate only those services required to fulfill the operational requirements of the system. They are initially hardened through the application of the policies established in the *Hardening Guide* and network scanning. Systems must be initially hardened before they are deployed and are regularly monitored. Hardening standards are established and available to system administrators in the *Hardening Guide*.

**Maintaining Multiple Environments**

Servers should be configured to support some combination of development or test environment, a quality assurance or preproduction environment and a production environment depending on the system owner’s needs. This practice allows developers greater access and flexibility to a given technology or application environment. The quality assurance or preproduction environment should mimic the production environment as much as possible and adhere to the same standards as the production environment. The production environment is isolated from development and test activities and is managed professionally.

**Research Environments**

The server recommendations outlined throughout this standard are highly recommended for use in the research environment. Consideration must be given to each individual standard point to determine if it is practical, feasible or financially available to research facilities to implement.

**Server Categories**

Within the University network, servers are classified and managed differently depending on the business, management, or academic needs and information access and storage requirements. There are different management requirements for each depending on access recovery times and data sensitivity.

**Server / Application Security Testing**

Systems are scanned with vulnerability assessment tools on initial configuration and on a recurring basis. Any issues identified are documented and resolved in accordance with current security practices. Vulnerability assessments should be performed minimally once per year.

**D. PROCEDURES, GUIDELINES & OTHER RELATED INFORMATION**

University Policy 3501 IT Access Control Security Policy
University Policy 3505 Security Policy
Information Security Program
IT Standard Desktop Management
### E. 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>Revised</td>
</tr>
<tr>
<td>January 2012</td>
<td>IT Policy Office</td>
<td>Updates to Maintain Multiple Environments, Research Environment, and Server Categories. Numbering revised</td>
</tr>
</tbody>
</table>