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.

Information Technology Standard: IT Facilities Security Standard
Reference Number: 6.1.0
Date of Current Revision or Creation: March 2012

A. PURPOSE

The purpose of this compliance standard is to establish the requirements for safeguard the physical facilities that house information technology equipment, systems, services, and personnel.

B. DEFINITIONS

IT Facilities is a static, mobile or portable facility (or facilities) or a location that contains Old Dominion University information technology equipment, systems, services, and personnel.

C. STANDARDS STATEMENT

Old Dominion University implements physical security practices to prevent unauthorized physical access, damage and interference to the institution’s premises and information. The protection provided should be commensurate with the identified risks.

Site Security

- Security perimeters of IT sites are clearly defined and controls depend on the requirements of the asset and the results of a risk assessment.
- The perimeters of the site should be physically sound and of solid construction.
- Doors should be suitably protected against unauthorized access with suitable control mechanisms.
- Physical security for offices, rooms and other facilities should consider all relevant health and safety standards.
Where applicable, sites should be unobtrusive and give minimum indication of their purpose.

Environmental Controls
- Physical barriers should provide environmental protection.
- Electric power, heating, fire suppression, ventilation, air-conditioning, and air purification are to be installed, as required by the IT systems and data.
- All fire doors are to be alarmed, monitored and tested in compliance with fire safety regulations.

Physical Access Controls
- Access to sites should be restricted to authorized personnel only.
- Physical access to essential computer hardware, wiring, displays, and networks by the principle of least privilege, where feasible.
- A system of monitoring and auditing physical access to sensitive IT systems is provided.
- The Information Security Officer (ISO) is to periodically review the list of persons allowed physical access to sensitive IT systems.

Working in Secure Areas
- Guidelines for working in secure areas should include controls for employees, contractors and third party users.
- Personnel should only be aware of activities on a need-to-know basis.
- Unsupervised working in secure areas should be avoided for safety reasons and to prevent opportunities for malicious activities.
- Vacant areas should be physically locked and periodically checked.
- Audio and video equipment is not allowed in secure areas without the authorization of the Information Security Officer.

Public Access, Delivery and Loading Areas
- Access points for deliveries and loading are to be controlled for unauthorized access.
- Incoming material should be inspected for potential threats before being moved to the point of use and handled in accordance with asset management procedures.

D. PROCEDURES, GUIDELINES & OTHER RELATED INFORMATION

Federal and State Law
University IT Policies
IT Policies and Standards

E. HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Responsible Party</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2008</td>
<td>ITAC/CIO</td>
<td>Created</td>
</tr>
<tr>
<td>October 2009</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2010</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>October 2011</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>Date</td>
<td>Department</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>March 2012</td>
<td>ITAC/CIO</td>
<td>Revised for working in secure areas and public access and delivery</td>
</tr>
<tr>
<td>December 2012</td>
<td>IT Policy Office</td>
<td>Numbering revision</td>
</tr>
</tbody>
</table>