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: Virus and Malicious Code Protection Standard
Reference Number: 05.4.0
Date of Current Revision or Creation: December 2012

A. PURPOSE
The purpose of this standard is to define the requirements to protect and defend the Old Dominion University network from the spread of a computer virus or other unintended or malicious destruction.

A. DEFINITIONS

Anti-virus software - A software package intended for the protection of technology resources both on and off-campus that is licensed by ODU for use by faculty, staff and students.

Virus – Files containing malicious software known to be intentionally destructive to technology resources.

B. STANDARDS STATEMENT

Virus Protection
Users will not willfully introduce virus-infected media or other foreign materials into any University systems without proper authorization and without using up-to-date, approved virus-scanning software.

Anti-Virus software will be made available to run on all University computers and on all computers connected to the network, including off-campus computers. Personally owned computers are also subject to compliance when connected to the network.

OCCS will monitor network activity and take appropriate action to control infection. Any server or client known to be an infecting agent will be disconnected and the user notified immediately and will be responsible for bringing the device into compliance.
**Malicious Code Protection**

Users will not intentionally develop or experiment with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.) and are prohibited from knowingly propagating malicious programs including opening attachments from unknown sources.

ODU will provide malicious program detection, protection, eradication, logging, and reporting capabilities and protection mechanisms for IT systems and users. Malicious program protection should eliminate or quarantine malicious programs that it detects; provide an alert notification; automatically and periodically runs scans on memory and storage devices; automatically scans all files retrieved through a network connection, modem connection, or from an input storage device; allow only authorized personnel to modify program settings; and maintain a log of protection activities.

**Disciplinary Action**

OCCS will monitor network activity and take appropriate action to control infection. Any server or client known to be an infecting agent will be disconnected and the user notified immediately. OCCS will work with users to solve the problem and bring the device into compliance.

Users who willfully disregard this standard are subject to disciplinary actions as provided for in other organizational employment and human resources policies.

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

Federal and State Law

**University IT Policies**

**IT Standards and Guidelines**

ISO 10.4.1 Controls Against Malicious Code

**D. HISTORY**

<table>
<thead>
<tr>
<th>Date</th>
<th>Responsible Party</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<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>October 2012</td>
<td>ITAC/CIO</td>
<td>Reaffirmed</td>
</tr>
<tr>
<td>December 2012</td>
<td>ITAC/CIO</td>
<td>Merged Virus Protection and Malicious Code Protection Standards Numbering revision</td>
</tr>
</tbody>
</table>