1. Overview
With the increased reliance on internet connectivity, *antivirus* software is necessary to protect a computer against viruses, worms and other types of malicious code. All computers connected to the *University network* must be running current *antivirus software*. In an effort to protect our computing environment, the *University of Arizona* provides *antivirus software* at no cost to all faculty, staff, and students for use on personal or *University* computers.

2. Purpose
The following guidelines will assist *University* faculty, staff, and students in obtaining and updating *antivirus software* to secure computers connected to the *University network*. Departments and individuals are encouraged to contact local computer support before implementing. These guidelines should not be used to hamper the procedures that may already exist.

3. Scope
These *antivirus software* guidelines apply to all computers connected to the *University network* for the transmission of electronic communications. This includes computers situated behind firewalls or NAT devices that are connected to the *University network* or are using a *VPN*.

4. Guidelines for Determining Which Sophos Product to Use
The *University of Arizona* offers a variety of *antivirus products*; in most cases, Sophos Remote Update is the preferred method of installing Sophos *Antivirus*.

- **Sophos Remote Update** offers the ability to automatically update and maintain Sophos *Antivirus software* on Microsoft Windows-based computers. Remote Update will install the Sophos *Antivirus* program, update it, and then continue to update Sophos automatically through network connections to a server located at CCIT.

- **Sophos *Antivirus*** is provided separately for users who cannot use Sophos Remote Update, either on computers which are not connected to the internet, or which are running different platforms. Sophos *Antivirus* requires a manual updating process.

5. Obtaining and Installing Sophos *Antivirus*

6. Other *Antivirus* Products
While Sophos is provided to the *University* community at no cost, some departments and individuals choose to use other *antivirus solutions*. *University* security standards require that all *antivirus* products be kept up-to-date with regular vendor updates. Refer to
vendor documentation or local computer support for instructions on maintaining alternative *antivirus* products.

**Related Guidance**

- Information Security Policy (IS-100)
- Information Security Terms Guideline (IS-G100)
- Minimum Security for Networked Devices Standard (IS-S602)
- Minimum Security for Networked Devices Implementation Guideline (IS-G602A)

All *italicized terms* used in this standard are defined in the Information Security Terms Guideline (IS-G100).

**Revision History**

<table>
<thead>
<tr>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Draft</td>
<td>5/25/06</td>
</tr>
<tr>
<td>Effective Date</td>
<td>5/27/08</td>
</tr>
<tr>
<td>Revision (only new numbering):</td>
<td>08/22/12</td>
</tr>
<tr>
<td>Effective Date:</td>
<td>9/17/12</td>
</tr>
</tbody>
</table>