Requirements for Securing a Windows 7 Workstation that Processes Confidential Information

Procedure | Informative
Version number: 1.0.0
Last Update/Review: 3 April 2013
Approved By: Ms. Sallie Wright, Assistant Vice President and Deputy CIO

Minimum requirements to ensure that your Windows 7 workstation is compliant with the University Information Protection and Access Policy.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Centrally managed McAfee Endpoint encryption (full disk encryption) will be used to protect confidential data on desktops, laptops, and removable drives.</td>
</tr>
<tr>
<td>2.</td>
<td>Workstations that store, process, and submit confidential data are subject to random Information Assurance Vulnerability Assessment (IAVA) scans.</td>
</tr>
</tbody>
</table>
| 3.           | Choose a secure password. Passwords should:  
- be at least ten characters long,  
- consist of mixed case (at least one each of upper and lower case),  
- contain at least one non-alpha character (such as a number or symbol),  
- be significantly different from prior passwords, and  
- be changed at least every 90 days.  
*Hint:* A strong password might look something like: P@$w0r$ |
| 4.           | Secure Administrator account.  
   a) Go to your Desktop.  
   b) Click Start.  
   c) Type in lusrmgr.msc in the search field.  
   d) Open the Users folder.  
   e) Right-click Administrator.  
   f) Select Rename.  
   g) Rename the administrator account.  
   h) Ensure the built-in administrator account has a strong password.  
   i) Review all members of the administrators group. If any account does not need administrator’s privileges, please remove that account from the administrator group. |
| 5.           | Install centrally managed antivirus software.  
   McAfee antivirus software can be obtained from your IT manager or the university download site (http://av.gsu.edu), and its use is mandated via the Anti-Virus Software Policy. Please update the antivirus software to the latest definition file and run full scans of your machine regularly. |
6. Install centrally managed firewall

McAfee Host Intrusion Prevention (HIPS) software can be obtained from your college/department technology representative. The software can also be requested from: http://technology.gsu.edu/technology-services/it-services/security/firewall/.

7. Critical software updates will be installed in a timely manner for software installed on the workstation.

   a) Go to your Desktop.
   b) Click Start.
   c) Click Control Panel.
   d) Click System and Security
   e) Under Windows Update, click Turn automatic updating on or off
   f) Select Install updates automatically (recommended)
   g) Click OK.

8. Operate an Operating System Screen Saver Password on the computer.

   a) Click Start.
   b) Click Settings.
   c) Click Control Panel.
   d) Click Appearance and Personalization
   e) Under Personalization, click Change screen saver.
   f) Check the On resume, display logon screen box.
   g) Fill in Wait X minutes (this is the number of minutes you want the computer to wait before displaying the screen saver).
   h) Click OK.

9. Turn on auditing.

   a) Click Start, click Control Panel, and then click Administrative Tools.
   b) Double-click Local Security Policy.
   c) In the left pane, double-click Local Policies to expand it.
   d) In the left pane, click Audit Policy to display the individual policy settings in the right pane.
   e) Double-click Audit objects listed below and change access accordingly:

<table>
<thead>
<tr>
<th>Event</th>
<th>Level of Auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account logon events</td>
<td>Success, failure</td>
</tr>
<tr>
<td>Account management</td>
<td>Success, failure</td>
</tr>
<tr>
<td>Logon events</td>
<td>Success, failure</td>
</tr>
<tr>
<td>Policy change</td>
<td>Success, failure</td>
</tr>
<tr>
<td>Privilege use</td>
<td>Success, failure</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------</td>
</tr>
<tr>
<td>System events</td>
<td>Success, failure</td>
</tr>
</tbody>
</table>

10. Configure Internet Explorer
   
a) Click on TOOLS.
b) Select INTERNET OPTIONS.
c) Click on the SECURITY tab.
d) Set Security Level for Internet Zone & Local Intranet to at least MEDIUM-HIGH.
e) Click on the PRIVACY tab.
f) Set the Privacy Setting to at least MEDIUM-HIGH.
g) Click OK.

11. Check the credentials of anyone asking for information about your computer.

12. With the exception of non-university Instant Messaging (IM), peer to peer (P2P), and Internet Relay Chat (IRC) software, users can install software/applications that have been approved by the organization’s technology representative and/or manager.

   a) Click Start, click Control Panel, double-click on Programs and Features.
b) Select the IM, IRC, or P2P software to be removed and click Uninstall.
c) Select yes in the warning popup.

13. In accordance with the principle of least privilege, a user should only have minimal user profile privileges on computers that are based on that user’s job necessities (default is to deny access).
14. File an Incident Report to report any suspicious activity on your machine by sending an email that contains the following information to help.gsu.edu.

a) Type "Security Incident - High Priority" in the subject line of the email.
b) Give the date the incident occurred.
c) Describe the incident.
d) Optional: If you know your IP address, or the IP address of your attacker, please include.
e) Provide your contact information such as your name, phone number, and department.

Help: If you have questions, or need assistance, please contact Information Security (security@gsu.edu) or the Help Center (404-413-4357, help@gsu.edu).