Best Practices Desktop Support

Configuration Management

Includes Restricted Data Settings

Version 5.20

April 20, 2006
# Table of Contents

Table of Contents ........................................................................................................................ ii
List of Tables ....................................................................................................................................... iii
Revision History ............................................................................................................................... iv

1.0 Overview ...................................................................................................................................... 5
2.0 Overview – Microsoft Windows Overview .................................................................................. 6
3.0 Asset Tagging ............................................................................................................................. 11
4.0 Appearance .................................................................................................................................. 11
5.0 Hardware Settings ....................................................................................................................... 12
6.0 Internet Settings ........................................................................................................................... 12
7.0 Security Settings .......................................................................................................................... 13
8.0 Network Settings ........................................................................................................................ 14
9.0 Software Settings ........................................................................................................................ 15
10.0 PC-Leland and PC-AFS Attribute – 5 – .................................................................................... 16
11.0 Security Settings ......................................................................................................................... 16
12.0 Miscellaneous Registry Changes Settings .................................................................................. 24
13.0 System Settings .......................................................................................................................... 27
14.0 Audit Policy settings .................................................................................................................. 30
15.0 Troubleshooting Settings .......................................................................................................... 30
16.0 Overview—Apple OSX ................................................................................................................ 32
17.0 Asset Tracking .......................................................................................................................... 35
18.0 Appearance Settings .................................................................................................................. 35
19.0 Hardware Settings ...................................................................................................................... 35
20.0 Internet Settings ........................................................................................................................ 36
21.0 Network Settings ........................................................................................................................ 37
22.0 Software Settings ....................................................................................................................... 37
23.0 Security Settings ........................................................................................................................ 37
24.0 System Preferences: Sharing ........................................................................................................ 39
25.0 System Settings .......................................................................................................................... 41
26.0 Troubleshooting ........................................................................................................................ 43

Appendix A Stanford University Web Favorites ................................................................................. 44
List of Tables

Table 1 Revision History .............................................................................................................................. iv
Table 2 PC Attribute Descriptions ........................................................................................................... 6
Table 3 PC Attributes ............................................................................................................................. 10
Table 4 Mac Attribute Descriptions ....................................................................................................... 32
Table 5 Apple-Macintosh Attributes ....................................................................................................... 34
Table 6 Stanford University Web Favorites ............................................................................................ 44
Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description/Reason</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-17-05</td>
<td>5.7</td>
<td>Miscellaneous changes from TS</td>
<td>TS/MC/BC</td>
</tr>
<tr>
<td>8-19-05</td>
<td>5.8</td>
<td>Modifications to document layout and wording</td>
<td>Michelle Collette</td>
</tr>
<tr>
<td></td>
<td>5.9-</td>
<td>Modifications to document layout and wording</td>
<td>Michelle Collette</td>
</tr>
<tr>
<td>10-04-05</td>
<td>5.10</td>
<td>Deleted section 9.3 from PC Attributes table, from 9.3 page 15, and Appendix B BigFix Enforced Settings table. Updated TOC, LOT</td>
<td>Bruce Campbell</td>
</tr>
<tr>
<td>11-23-05</td>
<td>5.11</td>
<td>BigFix info Appendix C</td>
<td>Tom Ostroff</td>
</tr>
<tr>
<td></td>
<td>5.12</td>
<td>Updated Header/footer, TOC</td>
<td>Bruce Campbell/Tony Silveira, Tom O.</td>
</tr>
<tr>
<td>11-30-05</td>
<td>5.13</td>
<td>Updated PC Attributes Key, section 3.1, 5.2, 5.4, 10.0, deleted section 11.25, updated section 11.15, 11.36, 12.9, 13.2, 15.1, 15.2, 15.4, 15.5, 15.6, Appendix A URLs, Appendix C, TOC, added Table of Figures, updated footers.</td>
<td>Bruce Campbell/Tony Silveira, Tom O.</td>
</tr>
<tr>
<td>1-12-06</td>
<td></td>
<td>Moved paragraph in section 24.1</td>
<td>Bruce Campbell</td>
</tr>
<tr>
<td>1-30-05</td>
<td>5.15</td>
<td>Added new Stanford Logo to header</td>
<td>Bruce Campbell</td>
</tr>
<tr>
<td>1-31-06</td>
<td>5.16</td>
<td>Removed logo from pages</td>
<td>Bruce Campbell</td>
</tr>
<tr>
<td>2-22-06</td>
<td>5.17</td>
<td>Verbiage change: “Category A Settings” to “Restricted Data”</td>
<td>Bruce Campbell</td>
</tr>
<tr>
<td>2-27-06</td>
<td>5.18</td>
<td>Added “Enforce” value: “1” if the DCM enforced settings will be maintained by BigFix (see column 4 in the “PC Attributes” chart, “to both PC and Mac sections</td>
<td>Bruce Campbell</td>
</tr>
<tr>
<td>3-20-06</td>
<td>5.19</td>
<td>Updated Appendix C</td>
<td>Tom Ostroff</td>
</tr>
<tr>
<td>4-21-06</td>
<td>5.20</td>
<td>Removed BigFix Text</td>
<td>Bruce Campbell</td>
</tr>
</tbody>
</table>

Table 1 Revision History
1.0 Overview

These Best Practices were developed by an ITSS working group sponsored by the ITSS Desktop Team, including representatives from the Windows Systems Team and Client Support. They are intended for any Stanford-owned laptop, desktop, or “tower” personal computer, running the Microsoft operating system.

The Best Practices will be adopted by ITSS and by their clients with support contracts. ITSS will encourage others Stanford University personnel to adopt them as well.

The following configuration settings were developed by ITSS for Stanford University-owned personal computers which will provide the following benefits:

1.1 Improve system security.

1.2 Improve computer system stability.

1.3 Improve the client experience by providing a consistent and predictable desktop environment.

1.4 Reduce the number of inconsistencies and unpredictability between computers, thereby improving help support tasks such as troubleshooting, computer setup, and computer redeployment.

1.5 Improve client efficiency by improving computer performance, and eliminating system activity that may interrupt the client’s work flow.

1.6 Configure each computer system and related application settings so that they more effectively interact with Stanford University Administrative Applications.

1.7 Provide the client sufficient freedom and access that will permit customization and personalization of their computing environment that will suit their individual tastes and meet their requirements.

1.8 Apply additional security settings to ensure compliance with the guidelines for desktops containing Restricted Data (information about Restricted Data may be found at: http://www.stanford.edu/services/securecomputing/dataclass.html).
2.0 Overview – Microsoft Windows Overview

The list is not all inclusive of all possible Microsoft Windows systems-settings. Many settings not discussed in this document, control aspects of the personal computing experience that are personal options left to the discretion of owners and users of the computer. For that purpose, this Best Practices document intentionally excludes settings that do not directly support the benefits listed above.

Windows Operating System Standards – No attempt is made in this document to define the minimum level of Windows OS for non-Restricted Data users. IMPORTANT - Windows XP with Service Pack 2 has been defined as the minimum Windows OS for desktops and laptops hosting Restricted Data.

2.1 Reference Notes Settings Attributes Table

<table>
<thead>
<tr>
<th>Attribute Reference Number</th>
<th>Attribute Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Existing Security Self-Help Item</td>
</tr>
<tr>
<td>2</td>
<td>Applies to new or redeployed computers</td>
</tr>
<tr>
<td>3</td>
<td>Applies to existing computers</td>
</tr>
<tr>
<td>4</td>
<td>Enforced setting (B=BigFix, G=GPOs)</td>
</tr>
<tr>
<td>5</td>
<td>Used for trouble shooting</td>
</tr>
<tr>
<td>6</td>
<td>User can undo (return to previous value)</td>
</tr>
<tr>
<td>7</td>
<td>To reflect Restricted Data settings</td>
</tr>
<tr>
<td>8</td>
<td>This is a security related setting</td>
</tr>
</tbody>
</table>

Table 2 PC Attribute Descriptions

a. The designated use of the attributes can be found in PC Attributes Table
### PC Attributes Key

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Set #</th>
<th>Setting Description</th>
<th>Attribute is Applicable to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>3.1</td>
<td>1</td>
<td>Asset Tagging</td>
<td>X</td>
</tr>
<tr>
<td>4.1</td>
<td>2</td>
<td>Web Favorites Stanford University (see Appendix C)</td>
<td>X</td>
</tr>
<tr>
<td>4.2</td>
<td>3</td>
<td>Add HelpSU to the Start Menu</td>
<td>X</td>
</tr>
<tr>
<td>4.3</td>
<td>4</td>
<td>Start Menu Run Command</td>
<td>X</td>
</tr>
<tr>
<td>4.4</td>
<td>5</td>
<td>Hide System Files and Folders</td>
<td>X</td>
</tr>
<tr>
<td>5.1</td>
<td>6</td>
<td>Power Management: Never Power-Off hard drives</td>
<td>X</td>
</tr>
<tr>
<td>5.2</td>
<td>7</td>
<td>Power Management: Disable Hibernation (Desktops)</td>
<td>X</td>
</tr>
<tr>
<td>5.3</td>
<td>8</td>
<td>AutoRun Set CDs and DVDS</td>
<td>X</td>
</tr>
<tr>
<td>5.4</td>
<td>9</td>
<td>Hardware Profiles</td>
<td>X</td>
</tr>
<tr>
<td>6.1</td>
<td>10</td>
<td>Default Browser is Internet Explorer</td>
<td>X</td>
</tr>
<tr>
<td>6.2</td>
<td>11</td>
<td>Internet Explorer (IE) Temporary Internet Files</td>
<td>X</td>
</tr>
<tr>
<td>6.3</td>
<td>12</td>
<td>Check for New Versions of Stored Pages</td>
<td>X</td>
</tr>
<tr>
<td>6.4</td>
<td>13</td>
<td>Default Email</td>
<td>X</td>
</tr>
<tr>
<td>6.5</td>
<td>14</td>
<td>Configure Email Client (Wizard Required)</td>
<td>X</td>
</tr>
<tr>
<td>6.6</td>
<td>15</td>
<td>Windows XP SP2 Pop-up blocker</td>
<td>X</td>
</tr>
<tr>
<td>7.1</td>
<td>16</td>
<td>Add [https://*].stanford.edu to the Intranet Zone (Permit pop-ups for Stanford https)</td>
<td>X</td>
</tr>
<tr>
<td>7.2</td>
<td>17</td>
<td>Auto Complete Settings</td>
<td>X</td>
</tr>
<tr>
<td>8.1</td>
<td>18</td>
<td>Configure DHCP for TCP/IP settings</td>
<td>X</td>
</tr>
<tr>
<td>8.2</td>
<td>19</td>
<td>TCP/IP setting: Turn-off Register this connection’s address in DNS</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>TCP/IP setting: M NETBIOS setting to “Default”</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>TCP/IP setting: Disable LMHOSTS Lookup</td>
<td>X</td>
</tr>
<tr>
<td>8.3</td>
<td>22</td>
<td>For Windows XP only, enable the XP Firewall</td>
<td>X</td>
</tr>
<tr>
<td>8.4</td>
<td>23</td>
<td>For Windows XP only, create entries for the specific Stanford Firewall Ports</td>
<td>X</td>
</tr>
<tr>
<td>8.5</td>
<td>24</td>
<td>Firewall exceptions created, but left closed</td>
<td>X</td>
</tr>
<tr>
<td>8.6</td>
<td>25</td>
<td>Automatically search for Network Folders and Printers</td>
<td>X</td>
</tr>
<tr>
<td>9.1</td>
<td>26</td>
<td>Pre-installed Software</td>
<td>X</td>
</tr>
<tr>
<td>9.2</td>
<td>27</td>
<td>Install the following ESS Software:</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>Symantec Anti Virus Corporate Edition</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>29</td>
<td>BigFix Patch Management Client</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>Security Self-Help Tool</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>31</td>
<td>PC-Leland</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>PC AFS</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>33</td>
<td>Secure FX</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>34</td>
<td>Secure CRT</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>35</td>
<td>Adobe Acrobat</td>
<td>X</td>
</tr>
<tr>
<td>9.3</td>
<td>36</td>
<td>Set Microsoft Office Macro Security to “Medium”</td>
<td>X</td>
</tr>
<tr>
<td>10.1</td>
<td>37</td>
<td>Reset and PC AFS settings</td>
<td>X</td>
</tr>
<tr>
<td>10.2</td>
<td>38</td>
<td>Reset system clock from Leland System time</td>
<td>X</td>
</tr>
<tr>
<td>11.1</td>
<td>39</td>
<td>Recommendation: Follow industry standards for robust passwords; establish secure local admin account for passwords.</td>
<td>X</td>
</tr>
</tbody>
</table>
## PC Attributes Key

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Set #</th>
<th>Setting Description</th>
<th>Attribute is Applicable to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>11.2</td>
<td>40</td>
<td>LMCompatibilitylevel</td>
<td>X</td>
</tr>
<tr>
<td>11.3</td>
<td>41</td>
<td>Password encryption</td>
<td>X</td>
</tr>
<tr>
<td>11.4</td>
<td>42</td>
<td>Screen Saver enabled</td>
<td>X</td>
</tr>
<tr>
<td>11.6</td>
<td>43</td>
<td>Recommendation: Rename Guest and Administrator Accounts</td>
<td>X</td>
</tr>
<tr>
<td>11.7</td>
<td>44</td>
<td>Administrator Account Rename</td>
<td>X</td>
</tr>
<tr>
<td>11.8</td>
<td>45</td>
<td>Windows Logon Window</td>
<td>X</td>
</tr>
<tr>
<td>11.9</td>
<td>46</td>
<td>Disable DCOM</td>
<td>X</td>
</tr>
<tr>
<td>11.10</td>
<td>47</td>
<td>Most current version of Symantec Antivirus must be installed</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>48</td>
<td>Enable Symantec Antivirus Live Update</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>49</td>
<td>Set Symantec Antivirus Live Update to Check for Virus Definition Updates Daily</td>
<td>X</td>
</tr>
<tr>
<td>11.11</td>
<td>50</td>
<td>Install BigFix Patch Management Client</td>
<td>X</td>
</tr>
<tr>
<td>11.12</td>
<td>51</td>
<td>Install PC-Leland</td>
<td>X</td>
</tr>
<tr>
<td>11.13</td>
<td>52</td>
<td>Restrict Anonymous Connections</td>
<td>X</td>
</tr>
<tr>
<td>11.14</td>
<td>53</td>
<td>File System Format Hard Drives as NTFS</td>
<td>X</td>
</tr>
<tr>
<td>11.15</td>
<td>54</td>
<td>Recommendation: Join the Windows Domain</td>
<td>X</td>
</tr>
<tr>
<td>11.16</td>
<td>55</td>
<td>Disable all High Risk Services</td>
<td>X</td>
</tr>
<tr>
<td>11.17</td>
<td>56</td>
<td>Disable AutoLogon</td>
<td>X</td>
</tr>
<tr>
<td>11.18</td>
<td>57</td>
<td>Disable Fast User Switching</td>
<td>X</td>
</tr>
<tr>
<td>11.19</td>
<td>58</td>
<td>Enable Windows Update</td>
<td>X</td>
</tr>
<tr>
<td>11.20</td>
<td>59</td>
<td>Set Windows Update to Check for Updates Daily</td>
<td>X</td>
</tr>
<tr>
<td>11.21</td>
<td>60</td>
<td>Disable IIS</td>
<td>X</td>
</tr>
<tr>
<td>11.22</td>
<td>61</td>
<td>Move Outlook and Outlook Express to the Restricted Zone</td>
<td>X</td>
</tr>
<tr>
<td>11.23</td>
<td>62</td>
<td>Do Not Share any Folders except the Administrative Shares</td>
<td>X</td>
</tr>
<tr>
<td>11.24</td>
<td>63</td>
<td>Disable Simple File Sharing</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>64</td>
<td>Enable Automatic Boot Disk Optimization</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>65</td>
<td>Recommendation: Limit the Membership of the Local Administrators Group</td>
<td>X</td>
</tr>
<tr>
<td>11.26</td>
<td>66</td>
<td>* Disable Remote Assistance and Close Port 3389 (if using WebX for remote support)</td>
<td>X</td>
</tr>
<tr>
<td>11.27</td>
<td>67</td>
<td>* Disable Remote Desktop</td>
<td>X</td>
</tr>
<tr>
<td>11.28</td>
<td>68</td>
<td>* Set Windows Script Security to Prompt Before Running Unsigned Script</td>
<td>X</td>
</tr>
<tr>
<td>11.29</td>
<td>69</td>
<td>* Set Windows Script Security to Prompt Before Running Unsigned Script</td>
<td>X</td>
</tr>
<tr>
<td>11.30</td>
<td>70</td>
<td>Recommend “Open With” Entries of Script File Extensions to Open With NotePad.EXE</td>
<td>X</td>
</tr>
<tr>
<td>11.31</td>
<td>71</td>
<td>Turn on “display all file extension”</td>
<td>X</td>
</tr>
<tr>
<td>11.32</td>
<td>72</td>
<td>Turn Off “Hide Extensions for Known File Types”</td>
<td>X</td>
</tr>
<tr>
<td>11.33</td>
<td>73</td>
<td>Disable Internet/Internet Explorer Password Caching</td>
<td>X</td>
</tr>
<tr>
<td>11.34</td>
<td>74</td>
<td>* Turn Off Internet Connection Sharing</td>
<td>X</td>
</tr>
</tbody>
</table>
### PC Attributes Key

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Set #</th>
<th>Setting Description</th>
<th>Attribute is Applicable to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.35</td>
<td>75.</td>
<td>Set &quot;Nolmhash&quot; registry item to 1</td>
<td>X X X</td>
</tr>
<tr>
<td>11.36</td>
<td>76.</td>
<td>Restrict Administrator login</td>
<td>X X X</td>
</tr>
<tr>
<td>11.37</td>
<td>77.</td>
<td>Disable Windows File Sharing</td>
<td>X X X</td>
</tr>
<tr>
<td>11.38</td>
<td>78.</td>
<td>Set Enforce Password History</td>
<td>X X X</td>
</tr>
<tr>
<td>11.39</td>
<td>79.</td>
<td>Set minimum password length</td>
<td>X X X</td>
</tr>
<tr>
<td>11.40</td>
<td>80.</td>
<td>Disable &quot;Store password using reversible encryption for all users in the domain.&quot;</td>
<td>X X X</td>
</tr>
<tr>
<td>12.2</td>
<td>82.</td>
<td>DHCP Router Discovery</td>
<td>X X X B</td>
</tr>
<tr>
<td>12.3</td>
<td>83.</td>
<td>Misc. Reg. Settings: Change AEDebug</td>
<td>X X X B</td>
</tr>
<tr>
<td>12.5</td>
<td>85.</td>
<td>Misc. Reg. Settings: Change Detect and Use Alternate Gateway</td>
<td>X X X B</td>
</tr>
<tr>
<td>12.6</td>
<td>86.</td>
<td>Misc. Reg. Settings: Change Enable Path MTU Discover</td>
<td>X X X B</td>
</tr>
<tr>
<td>12.7</td>
<td>87.</td>
<td>Misc. Reg. Settings: Change Name Release on Demand</td>
<td>X X X B</td>
</tr>
<tr>
<td>12.8</td>
<td>88.</td>
<td>Misc. Reg. Settings: Change Protect Against SYN Flood Attacks</td>
<td>X X X B</td>
</tr>
<tr>
<td>12.9</td>
<td>89.</td>
<td>Misc. Reg. Settings: Change TcpMaxHalfOpen</td>
<td>X X X B</td>
</tr>
<tr>
<td>12.13</td>
<td>93.</td>
<td>Limit Local Account Use of Blank Passwords to Console Logon Only</td>
<td>X X B G</td>
</tr>
<tr>
<td>13.1</td>
<td>94.</td>
<td>Set the SNTP to sync the computer time to time.stanford.edu</td>
<td>X X B</td>
</tr>
<tr>
<td>13.2</td>
<td>95.</td>
<td>Set Virtual Memory Paging to &quot;System Managed Size&quot;</td>
<td>X X</td>
</tr>
<tr>
<td>13.3</td>
<td>96.</td>
<td>* Turn Off System Restore</td>
<td>X X</td>
</tr>
<tr>
<td>13.4</td>
<td>97.</td>
<td>Startup and Recovery: Log System Failures</td>
<td>X X X X X</td>
</tr>
<tr>
<td>13.5</td>
<td>98.</td>
<td>Startup and Recovery: Turn Off Send Administrative Alerts</td>
<td>X X X X X</td>
</tr>
<tr>
<td>13.6</td>
<td>99.</td>
<td>Startup and Recovery: Enable Crash Dump</td>
<td>X X X X X</td>
</tr>
<tr>
<td>13.7</td>
<td>100.</td>
<td>Startup and Recovery: Crash Dump File Location = %SystemRoot%\MiniDump</td>
<td>X X X X X</td>
</tr>
<tr>
<td>13.8</td>
<td>101.</td>
<td>* Turn Off the &quot;Send to Microsoft&quot; Dialog on Errors</td>
<td>X X X</td>
</tr>
<tr>
<td>13.9</td>
<td>102.</td>
<td>Enable Clear Virtual Memory Pagefile when system shuts down</td>
<td>X X X</td>
</tr>
<tr>
<td>13.10</td>
<td>103.</td>
<td>Enable &quot;Do not display last user name in logon screen.&quot;</td>
<td>X X X</td>
</tr>
<tr>
<td>13.11</td>
<td>104.</td>
<td>Overwrite events as needed</td>
<td>X X X</td>
</tr>
<tr>
<td>14.0</td>
<td>105.</td>
<td>Audit policy settings</td>
<td>X X X</td>
</tr>
<tr>
<td>106.</td>
<td></td>
<td>Account management</td>
<td>X X X</td>
</tr>
<tr>
<td>107.</td>
<td></td>
<td>Directory service access</td>
<td>X X X</td>
</tr>
</tbody>
</table>
# PC Attributes Key

1. Existing Security Self-Help Item  
2. Applies to new or redeployed computers  
3. Applies to existing computers  
4. Enforced setting (B=BigFix, G=GPOs)  
5. Used for trouble shooting  
6. User can undo (return to previous value)  
7. Attribute 7 Restricted Data Settings  
8. This is a security related setting

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Set #</th>
<th>Setting Description</th>
<th>Attribute is Applicable to:</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>108. Logon events</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>109. Object access</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>110. Policy change</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>111. Privilege use</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>112. Process tracking</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>113. System events</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>114. Repair the TaskBar</td>
<td>115.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>115. Repair the Icon Cache</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>116. Repair the Office Shortcut Bar</td>
<td>5.3.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>117. Repair the Registry Editor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>118. Restore the Windows Explorer New Command</td>
<td>5.5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>119. Repair Internet Explorer Printing Errors</td>
<td>5.6.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 3 PC Attributes**
3.0 Asset Tagging

3.1 Asset Tagging (Setting # 1) – Attributes 2, 3, and 7 –

Enforced setting for asset tracking purposes, computers must contain the information in the registry that identifies the computer. The BigFix client software will be used to read this information in the Stanford University software and hardware database.

a. Place asset information in the registry key:
   1. `HKEY_LOCAL_MACHINE\Software\Stanford\DCM`

b. The information in the key shall include:
   1. Item: “PropertyTag,” value: The Stanford University Property Tag number (i.e. 176528).
   2. Item: “StanfordPC,” value: “0”. if the computer was not purchased by Stanford University (i.e., if it was purchased by a grant or owned by the individual), or “1” if the computer was purchased by Stanford University.

c. “Owner” value is the name of the individual or organization responsible for the computer.

d. “OnCampus” value: “1” if the computer is used on campus.

e. “Enforce” value “1” if the DCM enforced settings will be maintained by BigFix (see column 4 in the “Pc Attrituters” chart.

4.0 Appearance

4.1 Favorites – Attributes 2, 3, and 4 –

A list of commonly used Stanford Web sites will be placed in the Start + Favorites menu (see Appendix C).

4.2 Start Menu → HelpSU – Attributes 2, 3, and 4 –

A link to the HelpSU web site shall be added to the “All Users” Start Menu (HelpSU.url file added to:

a. `C:\Documents and Settings\All Users\Start Menu`

4.3 Start Menu → Run Command – Attributes 2 and 3 –

The “Run command” shall be available from the Start Menu.

4.4 Hidden Files and Folders – Attributes 2, 3, and 4 –

The computer shall be configured to hide those files and folders marked as “hidden.” These files shall not be accessed by the user, and their display clutters up Windows Explorer folder and file view. This configuration can be set by making the following registry change:

User Key:
`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`

Value Name: Hidden
Data Type: REG_DWORD (DWORD Value)
Value Data: 2
5.0 Hardware Settings

5.1 Power Management (Desktop Computers) – Attributes 2, 3, 5, and 6 –

For desktop computers, hard disks shall be set to “always remain on” (for laptop computers, this setting is left to user choice). Setting the hard drive to turn itself off after an idle period can adversely affect background applications that require disk access. This configuration can be set by changing the following registry entry.

User Key: [HKEY_CURRENT_USER\Control Panel\PowerCfg]
System Key: [HKEY_USERS\.DEFAULT\Control Panel\PowerCfg]
Value Name: CurrentPowerPolicy
Data Type: REG_SZ (String Value)
Data Value:

5.2 Hibernation shall be disabled for Desktop Computers. – Recommendation only: Hibernation can cause some applications to malfunction. It should be turned off for desktop computers.

5.3 Auto Run – Attributes 2, 3, 5, and 6 –

CDs and DVDs must be set to automatically start when loaded because most users are inexperienced with using Windows Explorer and the Run Command, and the methods for manually starting CDs and DVDs. This configuration can be set by changing the following registry entry:

User Key: [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
Value Name: CDRAutoRun
Data Type: REG_DWORD (DWORD Value)
Value Data: 1

5.4 Hardware Profiles, Attributes 2, 3, 7, and 8 –

Hardware profiles found under the option, “When Windows starts select the first profile list,” then set to 3. This option determines how long Windows will delay the boot process to allow the user to choose a hardware profile when starting up. This option is available only if multiple hardware profiles are available on the machine – ex. A laptop with a docking station will have a docked and an undocked profile and the profile cannot be automatically detected by Windows. Default is to wait 30 seconds for user input.

6.0 Internet Settings

6.1 Default Browser – Attribute 2 and 6

Internet Explorer (IE) shall be set as the default browser for all new computers and redeployed computers. Users can change this setting if they prefer a different browser.

6.2 Internet Explorer Temporary Internet Files – Attributes 2, 3, 5, and 6 –

The temporary internet files cache shall be set to (10 MB). To set this item to the minimum value, change the following setting for every user:

User Key:
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content]
And
6.3 “Check for Newer Versions of Stored Pages at every visit,” – Attributes 2, 3, 5, and 6 –

Some web-based applications require that new versions of web pages be downloaded every time the user visits the site. In addition, problems have been observed with Webauth and some Stanford University administrative applications if this setting is not set to “Every visit.” Set this to “Every visit” by making the following registry change for every user.

User Key:
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Content]
Value Name: Use CacheLimit
Data Type: REG_DWORD
Data Value: 1024

6.4 Default Email – Attribute 2 –

Outlook Express shall be set as the default email application on all new computers and redeployed computers. Although Eudora is available for download from the Essential Stanford Software site, it is no longer the recommended email software, and its use is discouraged.

6.5 Email Configuration – Attributes 2, 3, 5, and 6. –

Email programs shall be set to:

a. Incoming Mail Server: sunetid.pobox.stanford.edu
b. Outgoing Mail Server: smtp.stanford.edu
c. Account Name: sunetid
d. Use SSL

7.0 Security Settings

7.1 Windows XP SP2 Pop-up blocker– Attributes 2, 3, 5, and 6 –

Windows XP SP2 includes a pop-up blocker — i.e., software that prevents a web page from opening a separate browser window that commercial sites can fill with additional advertisements — the XP popup blocker is enabled by default. Most users prefer that pop-up blockers be enabled. However, this can be a challenge for users of the Stanford University Administrative applications, some of which require pop-up blockers to be disabled. The Best Practices requirement states if the user selects popup blocking, Stanford administrative pop-ups shall be the exception to the rule. Disabling “pop-ups” only for Stanford University administrative applications is accomplished by adding https://*.stanford.edu to the Internet Explorer Intranet Zone. This configuration shall be set for all users by adding the following registry items:

User Key: Create the key
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\stanford.edu]
Value Name: https
Data Type: REG_DWORD
Data Value: 1
7.2 Auto Complete Settings – Attributes 2,3,6,7, and 8 –

The auto-complete feature will store words that have been previously inserted into search boxes and forms at Web sites, such as search strings, names, email addresses, Website passwords and even credit card numbers. This behavior causes user frustration (for example, when an email address such as jdoe@stanford.edu is auto-entered into the Kronos login window), and presents a significant security vulnerability (for example, when credit card numbers or passwords are stored on the computer to be used in auto complete). Auto complete shall be set to allow the web address to be “auto completed,” and all other settings (forms, user names, passwords) shall be disabled for new and redeployed computers. Users shall be discouraged from changing this default. Change this setting for all users by making the following registry changes:

User Key: [HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]
Value Name: FormSuggest PW Ask
Data Type: REG_SZ (String)
Data Value: No
Value Name: Use FormSuggest
Data Type: REG_SZ (String)
Data Value: No
Value Name: AutoSuggest
Data Type: REG_SZ (String)
Data Value: Yes

8.0 Network Settings

8.1 DHCP – Attributes 2, 3, 5, 6, and 7 –
Computers shall be set to use Stanford DHCP. To do so, MAC Addresses, and the host name of the computer must be entered into Stanford’s NetDB database. However, if there is a compelling reason for the computer to use a static address, the following TCP/IP settings shall be set manually:

a. DNS Servers: 171.64.7.55, 171.64.7.77, 171.64.7.99
b. WINS Servers: 171.64.7.155, 171.64.7.177

8.2 TCP/IP Settings – Attributes 2, 3, 4, 6, and 7 –
All computers shall be set to the following TCP/IP configuration parameters:

a. Append primary and connection-specific DNS suffixes: On Append parent suffixes for the primary DNS suffix: Stanford.edu
b. Register this connection’s addresses in DNS: Off
c. NETBIOS Setting: Default. Category-A: Disable
d. Enable LMHOSTS Lookup: Disable

8.3 XP Firewall – Attributes 2, 3, 6, 7, and 8 –
The XP Firewall provides protection against common internet attacks, and must be enabled.

8.4 The following Stanford University specific ports must be opened – Attributes 2, 3, 5, 6, 7, and 8 –

a. BigFix: TCP 52311 and UDP 52311
b. ICMP: limit to “0” (echo reply)
8.5 The following firewall port exceptions must be created, but left closed unless the user needs to open them – Attributes 2, 3, 5, 6, 7, and 8 –
   a. Retrospect: TCP 497
   b. Retrospect: UDP 497
   c. FileMaker Pro: UDP 5003
   d. X-Windows: 6000

8.6 Automatically Search for Network Folders and Printers – Attributes 2, 3, 4, and 7
This setting controls whether Windows shall automatically attempt to locate available file shares and printers by crawling the local network. It is implemented by periodically scanning the computers on the network. During the scan, Windows identifies any newly-shared resources, such as a printer that has just gone online as a shared printer, or a folder that has just been shared. Network-crawling increases network traffic, and is a setting that has been disabled for all systems joining the Stanford WIN domain.

The Best Practice rule states that Network-crawling shall be disabled, and this is implemented by following registry changes:

   Key:
   [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
   Value Name: NoNetCrawling
   Data Type: REG_DWORD (DWORD Value)
   Value Data: 1

9.0 Software Settings

9.1 Pre-Installed Software – Attributes 2 and 7 –

9.2 The following Essential Stanford Software shall be installed on all new computers:
   a. Symantec Antivirus Corporate Edition
   b. BigFix Patch Management Client
   c. Security Self-Help Tool
   d. PC-Leland
   e. PC-AFS
   f. Secure FX
   g. Secure CRT
   h. Adobe Acrobat

9.3 Microsoft Office – Attributes 2, 3, 4, 7, and 8 –
Word, Excel, and PowerPoint shall have their macro security settings set to “Medium.” This selection causes the applications to prompt the user when unsigned macros are about to be executed. These settings require different registry entries for different versions of Microsoft Office, and will not be detailed in this document.
10.0 PC-Leland and PC-AFS Attribute – 5 –

10.1 Reset the PC-Leland and PC-AFS registry settings to the application defaults. PC-Leland and PC-AFS can experience problems if application registry settings become corrupted. Resetting the registry entries can quickly resolve some problems.

10.2 Attributes setting: Reset the system clock to the Leland system time (from the server time.stanford.edu). Setting the system time to the Leland network time resolves some common Kerberos ticket problems.

11.0 Security Settings

11.1 Passwords – Attributes 7 and 8 –

a. Security-related setting

1. It is critical that all user accounts have robust passwords, especially those accounts with Administrator privileges. Passwords must be at least 7-characters in length, contain both upper and lowercase characters, numbers, and not be words that appear in the dictionary.

2. Support organizations need access to Windows Local Administrator account names and passwords to perform routine maintenance and problem resolution activities. Organizations supporting large numbers of computers must deal with the challenge of maintaining secure Administrator account passwords on multiple computers. Although there are many effective high cost solutions (smart cards, and so on), there are no effective, secure low-cost solutions.

3. Some organizations have established a common password used for all Administrator accounts, and known by all support personnel. The problem with this approach is that sharing passwords is not a secure solution since the risk of losing control of the passwords increases dramatically as they are revealed to additional staff.

4. Other organizations have allowed local administrators to establish their own passwords for computers under their control. However, this makes succession planning difficult and has resulted in the extensive use of Linux based password hacking tools to reset the Administrator account when the support person that established the password leaves the organization without informing co-workers of the password.

5. Some organizations have assigned a null-password to the Administrator account to avoid this issue. Although using a null-Administrator password on Windows XP computers will automatically prevent network access using the Administrator account, unauthorized access remains possible from the console on computers that are not physically secured. Windows 2000 does not restrict remote access using null passwords. This is a significant security risk on an open-network like Stanford’s.

11.2 LMCompatibilityLevel – Attributes 1, 2, 3, 4, 7, and 8

The following registry entry shall be set to configure the “LMCompatibilityLevel” entry to the Stanford University standard, which restricts down-level authentication –.
11.3 Password Encryption – Attributes 7 and 8 –
Stanford is recommending a scheme to use a strong secret key and complex encryption to establish Administrator account passwords based on the host name of the computer. A secure web server will be used to store the encrypted passwords and secret key. When support personnel need to log on using the Administrator account, they will log on to the secure server, and enter the host name of the computer, and the server will then display the administrator password. This method will be piloted, and if successful, shall be implemented by ITSS for its contract clients.

11.4 Screen Saver – Attributes 2, 7, and 8 –
To promote desktop security, particularly in open environments, the Windows screen saver shall be enabled, initiating 30-minutes after the most recent keyboard/mouse activity, and requiring a password to unlock it.

11.5 Well-Known Local Accounts
Both the built-in “Guest” account and the built-in “Administrator” account shall be renamed to something other than “Guest” or “Administrator.”

11.6 Guest Account Rename – Attributes 1, 2, 3, 6, 7, and 8 –
   a. This change can easily be automated (the Security Self-Help tool currently does this) for the Guest account.

11.7 Administrator Account Rename – Attributes 7 and 8 – The Administrator Account is critical for computer support, and is often the only account available to the support professional requiring access to the computer for troubleshooting or system maintenance. This change cannot be automated for the Administrator account.
   a. If the Administrator Account is renamed, the Attributes recommendation is to record the name and keep it in a safe location for future reference. If the Administrator account gets renamed by the owner without informing the consultant, the consultant may be unable to assist the client unless the Administrator account name is available.

11.8 Windows Logon Window – Attributes 2, 3, 6, 7, and 8 –
By default, Windows XP will display a welcome screen at logon. This welcome screen displays the names of all local users of the computer. User IDs shall not be visible because a person with physical access to the computer can use the displayed user names to attempt unauthorized access. This feature is dependent on Fast User Switching. The Windows Welcome screen can not be disabled if Fast User Switching is enabled. To disable the welcome screen make the following changes (note that a reboot will be required for the change to take effect):

System Key: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]
Value Name: LogonType
Data Type: REG_DWORD (DWORD Value)
Value Data: 0
Delete the item “Background” in the
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon] registry key.

11.9 DCOM – Attributes 1, 2, 3, 6, 7, and 8 –
(Distributed Component Object Model) attracts Internet worms and permits
systems to be remotely compromised by malicious hackers

DCOM shall be disabled. Disable it with the following registry change:
System Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole]
Value Name: EnableDCOM
Data Type: REG_SZ (String Value)
Value Data: "N"

11.10 Symantec Antivirus – Attributes 2, 3, 4, 7, and 8 –
Stanford University has purchased a site license to Symantec Antivirus (SAV).

Symantec Antivirus shall be installed on all computers that are connecting to the
Stanford network. SAV shall be set to operate in “Real Time Protection” mode.
Live update shall be configured to check for virus definitions daily, during a time
when it is likely that the computer is on. This requires a number of registry
changes and will not be detailed in this document.

11.11 Operating System Patches – Attributes 1, 2, 3, 7, and 8 –
The BigFix patch management system shall be installed on all computers that
access Stanford’s network. Stanford University has purchased a site license for
BigFix.

11.12 PC-Leland – Attributes 1, 2, 3, and 7 – PC-Leland is a Stanford-specific software
package that provides secure authentication for access to university computing
resources restricted to Stanford affiliates use, such as Stanford electronic mail,
specialized electronic journals and databases on the Library’s web site, and so
on; and the ability to store and share files very easily on the Leland system.

PC-Leland shall be installed on all computers that access the internet through
Stanford University’s network –

11.13 Restrict Anonymous Connections – Attributes 1, 2, 3, 4, 7, and 8 –
The "restrict anonymous" registry setting controls whether or not an anonymous
user can connect to your PC and get a complete list of all the user accounts that
are on it. When a hacker becomes aware of user account names, it is that much
easier to breach systems. The best option for “Attributes” would be to provide no
information at all (a setting of “2”); however, that setting has some unintended
consequences that make it problematic. For Restricted Data computers, the
setting should be set to the most restrictive setting (Windows 2000:2, and
Windows SP; do not allow anonymous enumeration of SAM accounts and do not
allow anonymous enumeration of SAM accounts and shares.

a. The following registry entry shall be set to configure the “restrict
anonymous” entry to the Stanford University standard, which provides
some account information but not account names:

System Key:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA]
Value Name: RestrictAnonymous
Data Type: REG_DWORD (DWORD Value)
Value Data: 1
Category-A Value Data: 2

11.14 File System – Attributes 1, 2, 7, and 8 –

Hard drives shall be formatted with NTFS (New Technology File System, first introduced with Windows NT) instead of FAT (File Allocation Table). NTFS permits additional control over user's access privileges for specific files and folders. Anyone with a DOS boot diskette can walk up to a PC formatted with FAT and read everything on the drive that isn't encrypted.

11.15 Domain Membership – Attributes 1 and 7 –

Membership in a centrally managed Windows domain lessens the burden on individual users to maintain their computers' security. Some Schools and other groups at Stanford already have well-established domains, and there is an effort underway to provide the advantages of domain membership to a broader segment of the university community.

Whenever possible, computers shall join the central Stanford University Windows domain. Computers that contain Category A Data must join the Stanford Windows domain.

11.16 High Risk Services – Attributes 1, 2, 3, 6, 7, and 8 –

For computers, network services are the doorways into Windows 2000 and XP systems, so "eliminate all unnecessary services" is a time-honored commandment for protecting computers. Win2K comes with a lot of services enabled by default, many of which you don't need. Even if the service doesn't offer direct access to system resources, it might expose a system to buffer overflow attacks and denial of service (DoS) attacks.

The following list of services shall be disabled for all computers:

a. Windows 2000
   1 Alerter
   2 ClipBook
   3 Internet Connection Sharing
   4 Messenger
   5 NetMeeting Remote Desktop Sharing
   6 Network DDE
   7 Network DDE DSDM
   8 Remote Registry Service
   9 Routing and Remote Access
   10 Telnet
   11 HP Web Jetadmin

b. Windows XP
   1 Alerter
   2 ClipBook
11.17 Auto-Logon – Attributes 1, 2, 7, and 8 –

Auto-logon permits a user to log in to Windows without manually entering a password, a convenient feature but also a dangerous one. If you always have physical control of your PC, this may not be too dangerous; but with auto-logon enabled, anyone with physical access can access your Windows account. Worse still, the password for an account with auto-logon enabled may be saved in the Windows registry in an unencrypted form. By default, Windows XP will enable auto-login when the Administrator account has not been assigned a password.

Auto-logon shall be disabled. (A user may choose to re-enable it if appropriate.)

Auto-logon can be disabled by deleting the following registry entries

System Key: \[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\]
Value Names: AutoAdminLogon, DefaultPassword

11.18 Fast User Switching – Attributes 1, 2, 7, and 8 –

Fast User Switching allows you to have more than one user logged on to a computer at the same time with the ability to quickly switch among them. Although this may be convenient in some cases, it prevents the computer from joining a domain, and is not considered secure as single-use login.

Disable fast user switching on all new computers and redeployed computers by making the following registry change:

System Key: \[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\]
Value Name: AllowMultipleTSSessions
Data Type: REG_DWORD (DWORD Value)
Value Data: 0

11.19 Windows Update – Attributes 1, 2, 3, 7, and 8 –

Even though it is a Best Practices requirement that BigFix be installed for patch management, Windows Update shall also be used. Using both methods will not interfere with either, and will provide a backup for both. For registry change details, see: http://support.microsoft.com/?kbid=328010

11.20 Internet Information Server (IIS) – Attributes 1, 2, 7, and 8 –
Desktop computers shall not be running web servers of any sort, IIS (Internet Information Service) or otherwise. Web servers are the most frequently exploited systems on the Internet, and they represent a very high security risk.

Internet Information Server shall be disabled on all new computers and redeployed computers and clients shall be strongly encouraged to avoid its use unless they have a significant and compelling reason to use IIS.

11.21 Outlook or Outlook Express in Restricted Zone – Attributes 1, 2, 3, 6, 7, and 8 –

Some viruses can infect your system when you read email — they execute an ActiveX control within an email message. Theoretically, they can also exploit bugs in Java. The mail programs Outlook and Outlook Express shall be moved to the Internet Restricted Zone. The registry entries necessary to accomplish this are complicated and will not be included in this document.

11.22 Shared Folders – Attributes 1, 2, 7, and 8 –

New computers and redeployed computers shall not have any shares (shared folders) pre-defined. The only shares that shall be available are the administrative shares (C$, IPC$, ADMIN$).

11.23 Simple File Sharing – Attributes 1, 2, 7, and 8 –

Simple file sharing makes peer-to-peer file sharing easier by eliminating the requirement to protect files and folders by establishing local user accounts and setting file and folder access control lists. Unfortunately, it does this by using the local guest account to access all shared files and folders. Simple file sharing shall be strongly discouraged on an open network like Stanford’s.

a. New computers and redeployed computers shall have simple file sharing disabled. It is highly recommended that existing computers also have simple file sharing disabled whenever this is practical.

11.24 Automatic Boot Disk Optimization – Attributes 2, 3, 5, and 6 –

Automatic Boot Disk Optimization will defragment the pre-fetch files (C:\Windows\Prefetch) on boot up. Automatic Boot Disk Optimization shall be enabled for all Windows XP computers. This setting is accomplished by making the following registry entry:

System Key:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Dfrg\BootOptimizeFunction]
Value Name: Enable
Data Type: REG_SZ (String Value)
Value Data: (Y = enabled, N = disabled)

11.25 Administrators Group Accounts – Attributes 2, 7 and 8 – The number of accounts in the local Administrators group shall be kept to an absolute minimum. The only accounts listed in the local administrators group shall be:

a. Administrator
b. The Primary User (if the user is allowed administrator rights)
c. Domain Admins or OU Admins (if the computer is a member of a domain)

11.26 Remote Assistance – Attributes 2, 3, 6, 7, and 8 –

Remote Assistance shall be disabled and the remote assistance port (3389) shall not be left open for all clients supported by ITSS. For other organizations Remote Assistance shall be used rather than Remote Desktop for remotes.
desktop support activities. Remote assistance can be disabled by making the following change:

System Key:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
Value Name: fAllowToGetHelp
Data Type: REG_DWORD (DWORD Value)
Value Data: 0

11.27 Remote Desktop – Attributes 2, 3, 6, 7, and 8 –

Remote Desktop shall be disabled on all new computers and redeployed computers. If a user requires this functionality, they will be able to turn it on. Due to security concerns, its use shall be discouraged; but if it is used, special attention shall be paid to security issues (establishing robust passwords, and on). Remote Desktop can be disabled by invoking the following change:

System Key:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]
Value Name: fDenyTSConnections
Data Type: REG_DWORD (DWORD Value)
Value Data: 1

11.28 Windows Script Signature Security – Attributes 1, 2, 3, 6, 7, and 8 –

This setting defines whether or not trusted and un-trusted scripts shall be executed when using signature verification. Requiring a signature will cause the system to execute scripts only from verified authors.

This shall be set to direct the system to display a warning dialog showing the status of the script. Users will still be able to execute unsigned scripts if they choose to.

User Key: [HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script Host\Settings]
Value Name: TrustPolicy
Data Type: REG_DWORD (DWORD Value)
Value Data: 1

11.29 “Open With” – Attributes 2, 3, 6, 7, and 8 –

Change the file extension “open with” entries to use NotePad.exe to open all script file extensions. This will prevent the inadvertent running of malicious scripts in Windows Explorer. Modify the following extensions: .ws, .wsc, .wsf, .js, .vb, .vbe, .vbs.

Warning: This action will break existing scripts that may be in place for management, monitoring, or automation – including domain logon scripts. For existing scripts that are named with any of the file extensions that are listed here, users will need to preface the name of the script with the appropriate script host binary (cscript.exe or wscript.exe) in the call to execute the script.

The following registry entries control file associations:

Key:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\FileExtension\OpenWithList

Where FileExtension is the file extension with the period (i.e. .vbs)
Items:
MRUList ("a", "ab", "abc", etc.)
MRULetter (corresponds to one of the letters in the MRUList).
The Value of MRULetter shall be set to Notepad.exe.

11.30 Show All File Extensions – Attributes 1, 2, 3, 6, 7, and 8 –

By default, Windows hides the file extensions for known file types. This has been used by viruses to disguise malicious code as documents. For example, the file "readme.txt.exe" would be displayed as "readme.txt" if file extensions for known types are being hidden. To reduce this danger, the full file name, including the extension, shall be displayed. To show all file extensions: Search all keys in HKEY_CLASSES_ROOT for an entry called "NeverShowExt" — if it exists, delete it.

11.31 Hide Extensions for Known File Types – Attributes 1, 2, 3, 6, 7, and 8

Another registry entry that hides file types shall be set to display all file extensions:

User Key:
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\WindowsCurrentVersion\Explor er\Advanced]
Value Name: HideFileExt
Data Type: REG_DWORD (DWORD Value)
Value Data: 0

11.32 Internet and Internet Explorer Password Caching – Attributes 1, 2, 3, 4, 7, and 8

Password caching is the method that IE and internet applications use to store the user password on the computer so the user does not need to enter the password every time they visit the site. The problem with this approach is that the password is either stored in an unencrypted or in an encrypted form that is easily decrypted (see http://www.nirsoft.net/ for examples).

Caching IE and internet passwords shall be disabled for all new computers and redeployed computers, and users shall be strongly encouraged to avoid caching passwords. Make the following change to disable password caching for all users:

User Key:
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ Inte rnet Settings]
Value Name: DisablePasswordCaching
Data Type: REG_DWORD (DWORD Value)
Value Data: 1

11.33 Internet Connection Sharing – Attributes 1, 2, 3, 5, 6, 7, and 8 –

Internet connection sharing shall be turned off if it is on. ICS is inappropriate for use on the Stanford University network. It poses a significant data integrity risk and shall be disabled for all computers on campus.

11.34 Set "nolmhash" Registry item to 1 – Attributes 7 and 8 –

11.35 Restrict Administrator login. – Attributes 7 and 8 –

Add BUILTIN\Administrator to “deny access to this computer from the network," and "Deny logon through Terminal Services.

This setting should be maintained by applying a domain group policy.

11.36 Disable Windows File Sharing – Attributes 7 and 8 –
11.37 Set Enforce Password History – Attributes 2, 3, 7, and 8 –
This setting stores the previous X password hashes to prevent the user from re-
using the same password when their password expires and they are required to
change it, set it to 3.

11.38 Set minimum password length – Attributes 2, 3, 7, and 8 –
Minimum password length shall be a mixture of 7-characters.

11.39 Disable “Store password using reversible encryption for all users in the domain.”
(Local accounts when set on a machine) – Attributes 2, 3, 7, and 8 –.
This setting enables the Microsoft LSA provider to store a reversibly-encrypted
form of user’s passwords the next time they are changed. The option to store
reversibly encrypted passwords is only for support of authentication protocols
that do not support one-way hashing.

12.0 Miscellaneous Registry Changes Settings

12.1 Denial-of-Service Attack Protection – Attributes 1, 2, 3, 4, 7, and 8 –
Denial-of-service attacks are network attacks aimed at making a computer or a
particular service unavailable to network users.

The following settings can be used to increase the ability for Windows to defend
against these attacks when connected directly to the Internet:

System Key:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Param-
eters]
Value Name: EnableICMPRedirect, KeepAliveTime, PerformRouterDiscovery
Data Type: REG_DWORD (DWORD Value)
EnableICMPRedirect = 0
KeepAliveTime = 300,000
PerformRouterDiscovery = 0

12.2 DHCP Router Discovery – Attributes 1, 2, 3, 4, 7, and 8 –
The ICMP Router Discovery Protocol (IRDP) comes enabled by default for
Windows clients using DHCP. This can be a security issue because by spoofing
IRDP Router Advertisements, an attacker can remotely add default route entries
on a remote system.

12.3 AEDebug – Attributes 1, 2, 3, 4, 7, and 8 –
The “AEDebug” key is intended to allow an administrator to specify a remote
debugger that will be invoked as a troubleshooting measure in the event of a
system crash. The debugger runs in a highly-privileged state and unless
specifically required by the user (which is highly unlikely), shall be disabled:

System Key: [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\AEDebug]
Value Name: Auto
Data Type: REG_DWORD (DWORD Value)
Value Data: 0

12.4 Source IP Routing – Attributes 1, 2, 3, 4, 7, and 8 –
The IP-stack on any host (router or not) will drop packets with the source route
option set if DisableIPSSourceRouting is turned on. In most cases you do not
want a source routed packet to hit your host ever.
a. Setting DisableIPSourceRouting will enhance security on any system.

```
System
Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]
Value Name: DisableIPSourceRouting
Data Type: REG_DWORD (DWORD Value)
Value Data: 2
```

12.5 Detect and Use Alternate Gateway – Attributes 1, 2, 3, 4, 7, and 8 –

This setting specifies whether Windows shall automatically detect and use an alternate gateway in the event of transmitting a segment several times without receiving a response. This is a denial of service attack vulnerability.

a. Turn the setting off:

```
System
Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]
Value Name: EnableDeadGWDetect
Data Type: REG_DWORD (DWORD Value)
Value Data: 0
```

12.6 Enable Path MTU Discovery – Attributes 1, 2, 3, 4, 7, and 8 –

Enabling the setting causes TCP to attempt to discover the Maximum Transmission Unit (MTU or largest packet size) over the path to a remote host. By discovering the Path MTU and limiting TCP segments to this size, TCP can eliminate fragmentation at routers along the path that connect networks with different MTUs. This setting will improve network connectivity performance:

```
System
Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]
Value Name: EnablePMTUDiscovery
Data Type: REG_DWORD (DWORD Value)
Value Data: 0
```

12.7 Name Release on Demand – Attributes 1, 2, 3, 4, 7, and 8 –

The NetBIOS over TCP/IP (NBT) protocols are, by design, unauthenticated and therefore vulnerable to “spoofing.” A malicious user could possibly misuse the unauthenticated nature of the protocol to send a name-conflict datagram to a target computer to cause it to relinquish its name and stop responding to queries.

a. This setting will reduce the computer’s vulnerability to denial of service attacks:

```
System
Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]
Value Name: NoNameReleaseOnDemand
Data Type: REG_DWORD (DWORD Value)
Value Data: 1
```

12.8 Protect Against SYN Flood Attacks – Attributes 1, 2, 3, 4, 7, and 8 –

Windows includes protection that allows it to detect and adjust when the system is being targeted with a SYN flood attack (a type of denial of service attack based on incomplete handshake requests).
It shall be enabled, so that connection responses quickly time-out in the event of an attack.

System Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]
Value Name: SynAttackProtect
Data Type: REG_DWORD (DWORD Value)
Value Data: 2

12.9 TcpMaxHalfOpen – Attributes 1, 2, 3, 4, 7, and 8 –

SYN attack protection involves reducing the amount of retransmissions for the SYN-ACKS, which reduces the time resources have to remain allocated. The allocation of route cache entry resources is delayed until a connection is made. If synattackprotect = 2, then the connection indication to AFD is delayed until the three-way handshake is completed. Also note that the actions taken by the protection mechanism only occur if TcpMaxHalfOpen and TcpMaxHalfOpenRetried settings are exceeded.

System Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]
Value Name: TcpMaxHalfOpen
Data Type: REG_DWORD (DWORD Value)
Value Data: 100

12.10 TcpMaxHalfOpenRetried – Attributes 1, 2, 3, 4, 7, and 8 –

This value specifies how many connections the server can maintain in the half-open state even after a connection request has been retransmitted. If the number of connections exceeds the value of this entry, TCP/IP initiates SYN flooding attack protection. This entry is used only when SYN flooding attack protection is enabled on this server—that is, when the value of the SynAttackProtect entry is 1 and the value of the TCPMaxConnectResponseRetransmissions entry is at least 2.

System Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]
Value Name: TcpMaxHalfOpenRetried
Data Type: REG_DWORD (DWORD Value)
Value Data: 80

12.11 Change the Library Search Order – Attributes 1, 2, 3, 4, 7, and 8 –

This setting controls the order in which directories are searched for DLL (Dynamic Link Library) files. It ensures that a local DLL is used when a program is being run over a network, and it resolves issues where incompatible system DLL files are being loaded first.

System Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager]
Value Name: SafeDllSearchMode
Data Type: REG_DWORD (DWORD Value)
Value Data: 1

12.12 Disable the ADODB.Stream object – Attributes 1, 2, 3, 4, 7, and 8 –

An ADO stream object represents a file in memory. The stream object contains several methods for reading and writing binary files and text files. When this by-
design functionality is combined with known security vulnerabilities in Microsoft Internet Explorer, an Internet Web site could possibly execute scripts from the Local Machine zone

Using the ADODB Stream is not safe and shall be disabled.

System Key: \[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{00000566-0000-0010-8000-00AA006D2EA4}\]
Value Name: Compatibility Flags
Data Type: REG_DWORD (DWORD Value)
Value Data: 1024

12.13 Limit local account use of blank passwords to console logon only – Attributes 1, 2, 3, 4, 7, and 8 –

This controls whether or not local accounts with blank passwords can log on from the network. If this setting is enabled, local accounts with blank passwords cannot be used to connect to the machine from across the network, including via Windows Network as well as Terminal Services.

a. Accounts with blank passwords shall not be allowed remote access to the computer:

System Key: \[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]\Value Name: limitblankpassworduse
Data Type: REG_DWORD (DWORD Value)
Value Data: 1

13.0 System Settings

13.1 Simple Network Time Protocol (SNTP) – Attributes 2, 3, 4, and 5 –

Computer time is maintained by SNTP Window’s computers default to the time.windows.com server and OSX defaults to time.apple.com. If a computer is a member of the Stanford University Windows Domain, the SNTP is maintained by the domain controllers that sync their time to time.stanford.edu. To maintain consistency, all computers shall be set to sync time using time.stanford.edu. To set the SNTP server make the following registry entry (Windows computers):

System Key: \[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters]\Value Name: ntpserver
Data Type: REG_SZ (string)
Value Data: time.stanford.edu

13.2 Virtual memory paging – Recommendation only

Virtual memory paging shall be set to allow the system to size the page size (“System managed size”).

13.3 System Restore – Attribute 2 – 6

New XP computers or redeployed XP computers shall not use System Restore. It is ineffective, often does not work, and consumes unnecessary hard disk space and processor time. System Restore can be disabled by making the following registry entry:

System Key: \[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRestore\]
13.4 **Startup and Recovery – Attributes 2, 3, 4, 5, 6, and 7 –**

An event shall be written to the system log in the event of system failure. This setting is accomplished by making the following registry entry:

**System Key:**
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl]

**Value Name:** LogEvent
**Data Type:** REG_DWORD
**Value Data:** 1

13.5 **“Send an administrative alert” shall be disabled. – Attributes 2, 3, 6, and 7 –**

This setting is accomplished by making the following registry entry

**System Key:**
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl]

**Value Name:** SendAlert
**Data Type:** REG_DWORD
**Value Data:** 0

13.6 **Crash Dumps – Attributes 2, 3, 5, 6, and 7 –**

Crash Dumps enable the size of the dump file shall be set to “small memory dump”. This setting is accomplished by making the following registry entry –

**System Key:**
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl]

**Value Name:** CrashDumpEnabled
**Data Type:** REG_DWORD
**Value Data:** 3

13.7 **Crash Dump files shall be located in the default Windows location. – Attribute 2 –**

This setting is accomplished by making the following registry entry

**System Key:**
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl]

**Value Name:** MinidumpDir
**Data Type:** REG_SZ (String Value)
**Value Data:** %SystemRoot%\Minidump

13.8 **“Send to Microsoft” – Attributes 2, 3, and 6 –**

The “Send to Microsoft” dialog on application errors shall be disabled. This can be disabled by making the following registry entries:

**System Key:**
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting] Value Name: DoReport, ShowUI, IncludeKernelFaults, IncludeMicrosoftApps, IncludeWindowsApps
**Data Type:** REG_DWORD (DWORD Value)
**Value Data:** 0

13.9 **Enable Clear Virtual Memory Pagefile when system shuts down – Attributes 2, 3, 7, and 8 –**
During normal computer operations, data that is not being immediately used by active processes may be moved from memory to the system’s hard drive (paged) to free up physical memory. The pagefile is only accessible by the operating system, but may be accessed by 3rd-party tools if physical access is available to the machine while it is offline. To prevent this access, this setting causes the OS to write all ‘0’ to the pagefile when shutting down. Enabling this setting negatively affects system performance.

Registry:
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown = REG_DWORD 1

13.10 Enable “Do not display last user name in logon screen.” – Attributes 2, 3, 7, and 8 –

By default, the last logged on user name is filled in when the GINA (Graphical Identification and Authentication) dialog appears for the user’s convenience. This gives someone with console access to the machine a head start trying to break into the system by providing a valid user name. With this setting enabled, the dialog field appears blank.

Registry:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\dontdisplaylastusername = REG_DWORD 1

13.11 Event Viewer: Overwrite Events as Needed – Attributes 2, 3, and 7 –

Retention method determines how long events are kept in the event logs. If an event log fills up and the retention method does not allow any old messages to be aged out, then new messages will be lost.

a. GPO (Active Directory GPO only):
   1 Computer configuration\Windows Settings\Security Settings\Event Log\Settings for Event Logs\
      - Retention method for application log
      - Retention method for security log
      - Retention method for system log
   2 Option: Overwrite as needed
   3 Option: Overwrite by days
      - When setting this option, the retention period, in days, must also be set.
   4 Option: Do not overwrite events (clear log manually)

Registry:
HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\Retention = REG_DWORD 0
HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security\Retention = REG_DWORD 0
HKLM\SYSTEM\CurrentControlSet\Services\EventLog\System\Retention = REG_DWORD 0
Option: 0 = Overwrite as needed
Option: <numeric value> = Time (in seconds) to retain events
Option: 0xffffffff = Do not overwrite events
14.0 Audit Policy settings

14.1 Microsoft defines categories of events to be stored in the security event log. For each category, it can be selected to collect events on success or failure of actions in those categories, or both, or neither. – Attributes 2, 3, and 7

*The following attributes can be found under* Security Settings\Local Polices\Audit Policy

**NOTE – these Policies will not be set in the DCM Tool and are recommendations for all Restricted Data systems.**

- a. Account Logon Events: This category is for all account logon events inside a domain. **These events are not stored on the local machine, but are sent to the Domain Controllers for the domain in which the machine is a member. This will have no effect if the machine is not in a domain.** Audit account logon events: success, failure

- b. Account management: This category is for all account management activities (changes). Audit account management: success, failure

- c. Directory service access: This category is for all resource requests to the Active Directory. **This setting only affects Active Directory Domain Controllers.** Audit directory service access: success, failure

- d. Logon events: This category is for all authentication activity that occurs on a local machine. Audit logon events: success, failure

- e. Object Access: This category is for all authorization activities occurring on the local machine. Auditing must also be set on the individual resources (files, printers, registry keys, services, and so on.) for events to be logged. Audit object access: success, failure

- f. Policy change: This category is for all system policy management activities (changes). Audit policy change: success, failure

- g. Privilege Use: This category is for all actions that require system privileges (shutdown, creating shares, backup/recovery, and account management) Audit privilege use: success, failure

- h. Process Tracking: This category is for all process activities, including start/stop, loading/unloading DLLs, creating process objects, and so on. This category creates numerous events if running, and is not recommended unless troubleshooting an issue Audit process tracking: none

- i. System Events: This category is for system events (startup, page file expansion) Audit system events: success, failure

15.0 Troubleshooting Settings

Some changes to Windows computers are useful for troubleshooting, but do not improve the client experience, efficiency, or system stability. They can assist a computer support professional to solve common problems, or eliminate variables in a troubleshooting session. A troubleshooting tool could possibly incorporate these settings, automatically changing them to appropriate values whether or not they have caused or contributed to a problem. The following items shall be used by support personnel to quickly eliminate problems.

15.1 Repair the Taskbar – Attributes 5 –
If the taskbar has disappeared from the desktop or becomes hidden when the cursor moves near the taskbar, it may be due to a corrupt registry key. This setting will quickly repair this problem.

Delete the key:
```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StuckRects]
```

15.2 Repair the Icon Cache – Attributes 5 –

When the icon cache is corrupt, icons may appear incorrectly, or not at all. To fix this problem, delete the C:\Documents and Settings\username\Local Settings\Application Data\IconCache.db file (XP), or C:\Windows\Shell\IconCache file (Windows 2000).

15.3 Repair the Office Shortcut Bar – Attributes 3 and 5 –

The Office shortcut bar can become corrupt. This corruption can cause the application to function improperly. It can be repaired by deleting the registry key: HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Shortcut Bar and restarting the computer.

15.4 Repair the Registry Editor – Attributes 5 –

RegEdit.exe may not function correctly if its registry key becomes corrupt. This can be fixed by deleting the registry key:
```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit
```

15.5 Restore the Windows Explorer “New” Command – Attributes 5 –

Windows Explorer can lose the “New” command from the right-click context menu after program installations or upgrades. The following registry entry will restore the “New” command:

System Key:
```
[HKEY_CLASSES_ROOT\Directory\Background\shellex\ContextMenuHandlers\New]
```

Value Name: (Default)
Data Type: REG_SZ (String Value)
Value Data: {D969A300-E7FF-11d0-A93B-00A0C90F2719}

15.6 Repair Internet Explorer Printing Errors – Attributes repair setting 5

If printing from Internet Explorer produces blank pages or the pages that are printed are incorrectly displayed in print preview, the following registry entry might fix the problem:

User Key: [HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]

Value Name: Use StyleSheets
Data Type: REG_SZ (String Value)
Data Value: Yes
IE must be restarted after making this change.
16.0 **Overview—Apple OSX**

Apple Operating System Standards – No attempt is made in this document to define the minimum level of Apple Operating System for non-Restricted Data users. IMPORTANT – 10.3 (or greater) has been defined as the minimal level of OS for Apple desktops/laptops hosting Restricted Data

<table>
<thead>
<tr>
<th>Attribute Reference Number</th>
<th>Attribute Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Existing Security Self-Help Item</td>
</tr>
<tr>
<td>2</td>
<td>Applies to new or redeployed computers</td>
</tr>
<tr>
<td>3</td>
<td>Applies to existing computers</td>
</tr>
<tr>
<td>4</td>
<td>Enforced setting (B=BigFix, G=GPOs)</td>
</tr>
<tr>
<td>5</td>
<td>Used for trouble shooting</td>
</tr>
<tr>
<td>6</td>
<td>User can undo (return to previous value)</td>
</tr>
<tr>
<td>7</td>
<td>To reflect Restricted Data settings</td>
</tr>
<tr>
<td>8</td>
<td>This is a security related setting</td>
</tr>
</tbody>
</table>

*Table 4 Mac Attribute Descriptions*
## OSX Attributes Key

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Set #</th>
<th>Setting Description</th>
<th>Attribute is Applicable to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>17.1</td>
<td>120.</td>
<td>Asset Tag Information:</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Asset Tag Number (for equipment that is a capital asset)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Serial Number</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Stanford Owned flag</td>
<td></td>
</tr>
<tr>
<td>18.1</td>
<td>121.</td>
<td>Place an alias to the user’s home folder on the desktop and on the dock</td>
<td>X</td>
</tr>
<tr>
<td>18.2</td>
<td>122.</td>
<td>Finder opens to user’s home folder</td>
<td>X</td>
</tr>
<tr>
<td>18.3</td>
<td>123.</td>
<td>Show file extensions: Off</td>
<td>X</td>
</tr>
<tr>
<td>18.4</td>
<td>124.</td>
<td>Place the Stanford Favorites in the Dock</td>
<td>X</td>
</tr>
<tr>
<td>19.1</td>
<td>125.</td>
<td>Set hard disks not sleep when possible</td>
<td>X</td>
</tr>
<tr>
<td>20.1</td>
<td>126.</td>
<td>Make Internet Explorer the default browser</td>
<td>X</td>
</tr>
<tr>
<td>20.2</td>
<td>127.</td>
<td>Save downloaded files to the Desktop</td>
<td>X</td>
</tr>
<tr>
<td>20.3</td>
<td>128.</td>
<td>Block popups (browsers that support popup blocking)</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Allow popups for Stanford.edu</td>
<td>X</td>
</tr>
<tr>
<td>20.4</td>
<td>129.</td>
<td>Create a Wizard to configure Email settings for Stanford email</td>
<td>X</td>
</tr>
<tr>
<td>21.1</td>
<td>130.</td>
<td>Set up DHCP</td>
<td>X</td>
</tr>
<tr>
<td>21.2</td>
<td>131.</td>
<td>DHCP for acquisition</td>
<td>X</td>
</tr>
<tr>
<td>21.3</td>
<td>132.</td>
<td>Enable DHCP-retain old settings</td>
<td>X</td>
</tr>
<tr>
<td>21.4</td>
<td>133.</td>
<td>Disable AppleTalk</td>
<td>X</td>
</tr>
<tr>
<td>22.1</td>
<td>134.</td>
<td>Install the following ESS Software</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Symantec Anti Virus</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BigFix Patch Management Client</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Self-Help Too</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MacLeland and MacAFS</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internet Explorer</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Netscape</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adobe Acrobat</td>
<td>X</td>
</tr>
<tr>
<td>23.1</td>
<td>135.</td>
<td>Set the Office macro settings to “medium”</td>
<td>X</td>
</tr>
<tr>
<td>23.2</td>
<td>136.</td>
<td>Administrator accounts must be assigned a password</td>
<td>X</td>
</tr>
<tr>
<td>23.3</td>
<td>137.</td>
<td>Enable the firewall</td>
<td>X</td>
</tr>
<tr>
<td>23.4</td>
<td>138.</td>
<td>Open the S/Ident port (113), the BigFix port (52311)</td>
<td>X</td>
</tr>
<tr>
<td>23.5</td>
<td>139.</td>
<td>Require a password to wake from sleep or screen saver</td>
<td>X</td>
</tr>
<tr>
<td>23.6</td>
<td>140.</td>
<td>Screen Saver: Sleep after 20 minutes</td>
<td>X</td>
</tr>
<tr>
<td>23.7</td>
<td>141.</td>
<td>Disable auto logon</td>
<td>X</td>
</tr>
<tr>
<td>23.8</td>
<td>142.</td>
<td>Require password to unlock each secure system preference</td>
<td>X</td>
</tr>
<tr>
<td>23.9</td>
<td>143.</td>
<td>Install BigFix</td>
<td>X</td>
</tr>
<tr>
<td>23.10</td>
<td>144.</td>
<td>Symantec Antivirus shall be installed, and at the most current version</td>
<td>X</td>
</tr>
</tbody>
</table>
## OSX Attributes Key

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Set #</th>
<th>Setting Description</th>
<th>Attribute is Applicable to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>145.</td>
<td></td>
<td>Symantec AntiVirus LiveUpdate shall be enabled</td>
<td>X</td>
</tr>
<tr>
<td>146.</td>
<td></td>
<td>Symantec AntiVirus LiveUpdate shall be set to check for updates daily</td>
<td>X</td>
</tr>
<tr>
<td>23.11</td>
<td></td>
<td>MacLeland shall be installed</td>
<td>X</td>
</tr>
<tr>
<td>24.1 a</td>
<td></td>
<td>Turn off personal file sharing</td>
<td>X</td>
</tr>
<tr>
<td>24.1 b</td>
<td></td>
<td>Turn off Windows file sharing</td>
<td>X</td>
</tr>
<tr>
<td>24.1 c</td>
<td></td>
<td>Turn off file personal web sharing</td>
<td>X</td>
</tr>
<tr>
<td>24.1 d</td>
<td></td>
<td>Turn off remote login</td>
<td>X</td>
</tr>
<tr>
<td>24.1 e</td>
<td></td>
<td>Turn off FTP access</td>
<td>X</td>
</tr>
<tr>
<td>24.1 f</td>
<td></td>
<td>Turn off Apple Remote Desktop for all computers</td>
<td>X</td>
</tr>
<tr>
<td>24.1 g</td>
<td></td>
<td>Turn off remote Apple Events</td>
<td>X</td>
</tr>
<tr>
<td>24.1 h</td>
<td></td>
<td>Turn off printer sharing</td>
<td>X</td>
</tr>
<tr>
<td>24.2</td>
<td></td>
<td>Do not install Classic</td>
<td>X</td>
</tr>
<tr>
<td>24.3</td>
<td></td>
<td>Do not enable the root account</td>
<td>X</td>
</tr>
<tr>
<td>24.4</td>
<td></td>
<td>Disable Fast User Switching</td>
<td>X</td>
</tr>
<tr>
<td>24.5</td>
<td></td>
<td>Display the user name and password in the logon screen</td>
<td>X</td>
</tr>
<tr>
<td>24.6</td>
<td></td>
<td>Check for software updates every day</td>
<td>X</td>
</tr>
<tr>
<td>24.7</td>
<td></td>
<td>Install the OSXAutoUpdater</td>
<td>X</td>
</tr>
<tr>
<td>25.1</td>
<td></td>
<td>Format hard disks to HFS+</td>
<td>X</td>
</tr>
<tr>
<td>25.2</td>
<td></td>
<td>Do not log out after x minutes of inactivity</td>
<td>X</td>
</tr>
<tr>
<td>25.3</td>
<td></td>
<td>File Vault: Turn off</td>
<td>X</td>
</tr>
<tr>
<td>25.4</td>
<td></td>
<td>File Vault: Use PASSWRD WEB password for a File Vault password (for data recovery)</td>
<td>X</td>
</tr>
<tr>
<td>25.5</td>
<td></td>
<td>Energy Saver (Desktops): Never put the computer to sleep</td>
<td>X</td>
</tr>
<tr>
<td>25.6</td>
<td></td>
<td>Energy Saver (Desktops): Put the display to sleep after 30 minutes</td>
<td>X</td>
</tr>
<tr>
<td>25.7</td>
<td></td>
<td>Show warning before emptying the trash</td>
<td>X</td>
</tr>
<tr>
<td>25.8</td>
<td></td>
<td>Set the SNTP to sync the computer time to time.stanford.edu</td>
<td>X</td>
</tr>
<tr>
<td>26.1</td>
<td></td>
<td>Delete Temp Files (/tmp/###)</td>
<td>X</td>
</tr>
<tr>
<td>26.2</td>
<td></td>
<td>Reset the MacLeland and MacAFS settings back to the defaults</td>
<td>X</td>
</tr>
<tr>
<td>26.3</td>
<td></td>
<td>Reset the system clock to the Leland network time</td>
<td>X</td>
</tr>
</tbody>
</table>

Table 5 Apple-Macintosh Attributes
17.0 Asset Tracking

17.1 Stanford-owned Macintosh computers shall contain information that identifies the computer for asset tracking. The BigFix client software will be used to read this information in the Stanford University software and hardware inventory database. – Attributes 2, 3, and 7 –

Asset information shall be placed in the Mac. The information contained in that key must include:

- Item: “PropertyTag,” value: The Stanford University Property Tag number (i.e. 176528).
- Item: “StanfordPC,” value: False if the computer was not purchased by Stanford University (i.e., if it was purchased by a grant or owned by the individual), or True if the computer was purchased by Stanford University.
- “Enforce” value “1” if the DCM enforced settings will be maintained by BigFix (see column 4 in the “Pc Attributers” chart.

18.0 Appearance Settings

18.1 Place an alias to the user’s home folder on the desktop and the dock – Attributes 2 and 3:

Without these aliases, a former OS 9 user new to OS X usually has difficulty locating, and hence appreciating the value of the home directory. The aliases encourage the user to use the home folder (and sub-directories) as the primary location for personal data files.

~/Library/Preferences/com.apple.dock.plist

18.2 Finder windows open to Home-Folder – Attributes 2 –:

By default, the system setting when the operating system is initially installed, a new Finder window will open to the user’s home folder. This option will assist the user in keeping files stored in the home directory. This control is set in the Finder’s Preferences – in Finder, it is under the Finder menu.

~/Library/Preferences/com.apple.finder.plist

18.3 Show file extensions: Off – Attributes 2 –

By default, Mac OS X does not display file extensions on file names. Whether or not to modify is at the user’s discretion.

~/Library/Preferences/.GlobalPreferences.plist

18.4 Place the Stanford favorites in the dock. – Attributes 2 and 3 –

A set of Stanford favorite websites shall be added to the Dock, thus making it easier for the user to access a commonly used website with a single motion. The Stanford favorites (see Appendix B) will be placed in the user’s Library folder (~Library/Favorites). Additionally, an alias to the Favorites will be created by dragging the Stanford Favorites folder from the Finder to the lower portion of the Dock.

~/Library/Preferences/com.apple.dock.plist.

19.0 Hardware Settings

19.1 Set Hard Disks to Remain On – Attributes 2, 3, 5, 6, and 7 –
For desktop computers, hard disks shall be set to always remain on (for laptops, this setting is left to the user’s discretion). Setting the hard drive to turn itself off after an idle period may adversely affect background applications that require disk access.

20.0 Internet Settings

20.1 Default Browser = Internet Explorer – Attributes 2 –

Internet Explorer (IE) shall be set as the default browser for all new computers and redeployed computers. Users can change this if they prefer a different browser, but since IE is Stanford University's preferred browser, it shall be the default browser for all new Macintosh computers. Note that automating this change requires numerous configuration changes — many file extension associations must change.

20.2 Save downloaded files to the Desktop – Attributes 2, 3, 5, and 6 –

When files are downloaded from websites, users often have trouble initially locating the files placed on the Mac. Setting the desktop to be the destination for each browser maintains consistency with previous Mac operating systems. This setting is separately applied for each browser.

Safari: ~/Library/Preferences/com.apple.safari.plist
IE: Set via InternetConfig preferences within IE.
Netscape: ~/Library/Preferences/com.netscape.mozilla.plist

20.3 Block non-Stanford pop-ups (if supported by browser) – Attributes 2, 3, 6, and 8 –

Pop-up windows that appear during web-browsing are, in most cases, advertisements from commercial websites; and usually, no harm is done by suppressing them. Some browsers provide that capability, and it is a Best Practice to take advantage of it. This must be set individually for each browser that supports this option.

a. Some Stanford administrative applications with web interfaces do use pop-up windows, and need to be treated as exceptions. Some browsers support an exception list that allows popups from specified sites; for Stanford administrative applications, that site is secureweb.Stanford.edu.

Safari: ~/Library/Preferences/com.apple.Safari.plist
[Netscape:]

Netscape: ~/Library/Mozilla/Profiles/default/<profile>/hostperm.1

20.4 Create a wizard to configure email settings for Stanford email – Attributes 2, 3, 5, and 6 –

The purpose of this tool is to quickly apply known configuration settings to one or more of the ‘supported’ email clients installed on the system. The information necessary to configure a single email client is generally the same for most email clients. Only the files the settings go into are different, (e.g. outgoing mail server, incoming mail server, user id, and so on). This tool will allow support personnel
to quickly configure a system regardless of the email client choice made by the end user. A consultant could use this tool to reliably reset an email client to appropriate settings without having to try looking at every setting to see whether one or more are incorrectly configured.

21.0 Network Settings

21.1 Setup DHCP

21.2 DHCP for acquisition – Attributes 2 and 3 – All systems shall employ TCP/IP settings. This setting is made in the Network pane of System Preferences.

21.3 Enable DHCP and retain old settings – Attributes 5 and 6 – A troubleshooting consultant’s tool shall retain the old settings (perhaps a manual IP entry) so that it can undone.

a. Changes are recorded in:
   /Library/Preferences/SystemConfiguration/preferences.plist for each Ethernet device in the following setting:

21.4 Disable AppleTalk – Attribute 2 –

21.5 Unless necessary and within the local subnet AppleTalk shall be disabled. SUNet no longer routes AppleTalk between subnets. If AppleTalk is used within the subnet, plans are being made to move those services to other, supported protocols.

/Library/Preferences/SystemConfiguration/preferences.plist

22.0 Software Settings

22.1 Install ESS software required by most users, which is available from (http://ess.stanford.edu). Additionally, the standard Safari web browser that comes with OS X, Internet Explorer and Netscape are required for running the administrative applications Oracle Financials and Kronos, respectively.

a. Symantec AntiVirus Attributes 1, 2, 7, 8
b. BigFix Patch Management Client• Attribute 2
c. Security Self-Help Tool Attribute 2
d. MacLeland and MacAFS Attributes 1, 2, 7, 8
e. Internet Explorer Attributes 1, 2
f. Netscape Attribute 2
g. Adobe Acrobat Attribute 2

23.0 Security Settings

Note: BigFix client not yet available for the Mac.

23.1 Set the Office macro settings to “Medium” – Attributes 2, 3, 7, and 8 – Macros in Microsoft Office programs are a well-known tool for malicious hackers, hiding destructive code that can be sent into execution by a program unknown to the user. This office setting assists in blocking these types of problems, although a more secure (but intrusive) setting is available. This is set per office application (Word, Excel, and so on) in the application preferences.

23.2 Assign Passwords to All Administrator Accounts – Attributes 2, 3, 7, and 8 –
Because Administrator accounts on a Macintosh can read, write, or delete any data on that Macintosh all Administrator accounts shall have a password.

23.3 Enable the firewall – Attributes 2, 3, 6, and 8 –

All OS X systems shall use the operating system firewall found in the Firewall sub-panel of the Sharing pane of System Preferences. Use of Firewall will significantly reduce the vulnerability of attacks from external sources. Only ports necessary for system operations shall be opened.

/Library/Preferences/com.apple.sharing.firewall.plist

23.4 A troubleshooting tool for consultants would likewise open these ports on a user’s machine – Attributes 3, 5, 6, and 8 –

/Library/Preferences/com.apple.sharing.firewall.plist

23.5 Require a password to wake from sleep or screen saver

To promote desktop security, particularly in open environments, the Macintosh screen saver shall require a password to unlock it – Attributes 2, 7, and 8 –

Users make changes to these settings in the Security system preference.

~/Library/Preferences/ByHost/com.apple.screensaver.<mac addr>.plist

23.6 Screen Saver: Activate after 20 minutes – Attributes 2, 7, and 8 –

Used in conjunction with requiring passwords to unlock the screen saver (see below), having the screen saver activate at 20-minutes of inactivity increases the security of the system. This setting is found in the Energy Saver system preference. Users shall be encouraged to lower the time if comfortable with less, but twenty minutes is an appropriate default in most Stanford business settings.

~/Library/Preferences/ByHost/com.apple.screensaver.<mac addr>.plist

23.7 Disable autologin – Attributes 2, 7, and 8 –

Located in the Login Options of the Accounts system preference and in the Security system preference, auto-login shall be disabled. With the setting enabled, a simple reboot makes the user’s files (including downloaded email) and applications (as well as those of anyone else with an account on the computer if the auto-login account belongs to a user with administrative privileges) available to anyone pushing the power button.

Requiring all users to manually login improves the security of the system.

/Library/Preferences/com.apple.loginwindow.plist

23.8 Require a password to unlock each secure system preference – Attributes 2, 7, and 8 –

This item, also in the Security system preference, shall be the default selection. Enabling this will reduce the number of inadvertent changes to system preferences the might affect operation and performance.

/Library/Preferences/GlobalPreferences.plist

23.9 Install BigFix – Attributes 2, 3, 7, and 8 –

Currently, under development for the Macintosh, BigFix will automatically install software patches, generally overnight, without user intervention as Software Update does. This is a placeholder for details when it is released. See also OS X Auto-Updater, discussed later.
23.10 Install Symantec Antivirus and Use Live Update Daily – Attributes 2, 3, 4, 7, and 8 –

Mentioned earlier under “II.6 Software,” Symantec Antivirus shall be installed on all computers connecting to the Stanford network. The software shall be configured to have the Live Update feature check for daily updates to virus definitions, at a time when the computer is likely to be on (the check cannot occur if the computer is not on).

23.11 Install MacLeland – Attributes 2, 3, 7, and 8 –

Previously mentioned, under “II.6 Software,” MacLeland shall be installed on all computers connecting to the Stanford network. It provides authentication support for Stanford network services, and through its separately installable MacAFS (OpenAFS) software, provides access to Stanford’s AFS file system.

24.0 System Preferences: Sharing

24.1 The following 8 settings appear in the Services sub-panel of the Sharing pane of System Preferences. Each is a system-level setting that turns on the service for all the computer’s users. Each requires administrator access to make changes. Actual settings are saved in /Library/Preferences/com.apple.sharing.firewall.plist.

Due to constraints in the base operating system these settings cannot be programmatically set by the DCM tool (OSX 10.4.4 and earlier). After running the tool you must manually set these in System Preference → Sharing → Services

   a. Turn off Personal File Sharing – Attributes 2, 7, and 8 –

      1 For security reasons, a new or redeployed computer shall not start up with personal file sharing (via Apple File Protocol, AFP) enabled. (As is the case with most of these Sharing preferences, the user receiving the new computer is likely to assume, and shall be able to assume, that no basic security vulnerabilities are present that could be removed during the initial configuration.)

   b. Turn-off Windows File Sharing – Attributes 2, 7, and 8 –

      1 Windows file sharing shall not be enabled on a new or redeployed computer. Windows file sharing allows file sharing via SMB.

   c. Turn-off Personal Web Sharing Attributes 2, 7, and 8 –

      Generally, due to security vulnerabilities, desktop computers shall not be running web servers. Web servers are the most frequently exploited systems on the Internet, and they represent a high security risk. Stanford provides a robust and universally accessible web storage facility in AFS that is sufficient for most users for Stanford business.

      1 Personal web sharing shall not be enabled on a new or redeployed computer.

   d. Turn off Remote Login – Attributes 2, 7, and 8 –

      1 Remote login allows remote access via an encrypted TCP/IP connection using the SSH protocol. Remote login shall not be enabled on a new or redeployed computer.

   e. Turn off FTP Access – Attributes 2, 7, and 8 –
This setting allows users of other computers to exchange files with the computer using FTP applications. FTP shall not be enabled on a new or redeployed computer.

f. Turn off Apple Remote Desktop client—Attributes 2, 3, 6, 7, and 8—

Apple Remote Desktop (ARD) client allows remote users to connect to the Mac. Unlike SSH, ARD allows access via the graphical user interface. ARD shall not be enabled on a new or redeployed computer. ITSS consultants who use ARD to gain access to a user’s Mac as part of assisting a user can request the user turn ARD on, and then turn it off once the consulting is over.

2 −Disabling Apple Remote Desktop (ARD)−Attributes 3, 6, and 8—A consulting tool shall turn off ARD under the assumption that the user has forgotten to turn it off after a prior consultation. If it does get turned off, it shall be pointed out to the user that ARD has been disabled−after all, ARD is software a user could own and use for his own purposes, and finding it has been disabled when trying to remotely access the machine will be upsetting to the user.

g. Turn off Remote Apple Events—Attributes 2, 3, 6, 7, and 8—

This is a seldom used, legacy technology that has been replaced by other, more secure remote connectivity tools. Having it enabled, unless specifically used, increases the vulnerability of the system to external compromise.

The setting for Remote Apple Events shall not be enabled on a new or redeployed computer.

h. Turn off Printer Sharing—Attributes 2, 3, 6, 7, and 8—

Printer sharing allows a locally connected printer to be shared via the network. It shall not be enabled on a new or redeployed computer.

24.2 Do not install OS 9 / Classic−Attributes 2, 7, and 8−

OS 9 AKA, Classic shall not be installed unless necessary. It does not support directory and file permissions. It is possible to boot into Classic and have root-level access to all HFS+ partitions. Newer Macintoshes (some G4s and later) do not allow booting into OS 9, so this vulnerability will decrease over time as new machines replace old ones.

24.3 Do not enable the root password—Attributes 2, 7, and 8—

Enabling the root password enables the super-user account also known as root. Anyone who knows the username root and its password has access to all files, programs, and processes on the computer. A hacker will need to know both the account name and the password to gain access, but knowing the account name root gets the hacker halfway there. Keeping the super-user account disabled removes even that slight advantage to the hacker.

From the perspective of convenience for the computer’s owner, all administrator accounts have the ability to use the ‘sudo’ command on the command line interface. This allows them to perform most system-level operations without exposing the system to external attack by enabling the root account.

This option is configurable through NetInfo Manager in /Applications/Utilities.
24.4 Disable Fast User Switching – Attributes 2, 3, 6, 7, and 8 –

Fast user switching allows multiple users to be concurrently logged on to the system. Although convenient, in some cases, it is inconsistent with the campus web authentication system, and one user’s data could potentially be hacked by others concurrently logged on. This setting is found in the Login Options of the Accounts system preference.

/Library/Preferences/GlobalPreferences.plist

24.5 Require entry of the user name in the login screen – Attributes 2, 3, 6, 7, and 8 –

The login screen for OS X can ask for a user by either providing a simple entry field where the username is typed or by showing a pick-list of enabled users on the computer. The latter choice provides a hacker with one piece of the two required to break into the computer, making it the less secure choice.

a. The user shall be required to type the username at login. This setting is found in the Login Options of the Accounts system preference.

/Library/Preferences/loginwindow.plist

24.6 Check for software updates daily – Attributes 2, 3, 7, and 8 –

a. Software Update, a feature of OS X that checks for updates to various Apple software components, shall be set to check for them daily since they often include security patches. Enabling Software Update facilitates patching that requires user intervention. This setting is found in the Software Update system preference. If BigFix is used for system management, this setting can be turned off, though, there is no harm in running both.

~/Library/Preferences/com.apple.scheduler.plist

24.7 Install OSXAutoUpdater – Attributes 2, 3, 7, and 8 –

a. Currently under development in ITSS, the OSXAutoUpdater wraps around OS X’s Software Update program and installs software patches automatically, generally overnight, without requiring user intervention as Software Update does. BigFix may do this on the Mac too, but the client is not yet ready for the Mac. Hence, to further enhance system security through patch maintenance, the OSXAutoUpdater shall be installed and functional.

/Library/Management/OSXAutoUpdater/
et/crontab

25.0 System Settings

25.1 Format hard disks HFS+–Attributes 2 –

a. Disk partitions shall be formatted as HFS+ unless local circumstances dictate otherwise. Doing so ensures the highest level of compatibility with current Mac applications.

b. Tool design notes – Attributes 2 and 5 – If partitions are not formatted with the HFS+ format, an informational warning shall be displayed to the consultant by consultant tools.
25.2 Do not log out after x minutes of inactivity – Attributes 2 –

   a. The Mac can be configured to log out the current user if no activity is
detected for a specified number of minutes. Unless a specific reason
exists (such as a machine shared by multiple users), it is not necessary to
set auto logout. For a single-user machine, the same measure of security
can be achieved by having the screen saver automatically start after a
certain interval and then requiring a password to unlock the screen saver.

   /Library/Preferences/GlobalPreferences.plist

25.3 Turn off File Vault – Attributes 2 –

File Vault encrypts the user’s home directory and all its subdirectories with the
user’s login password. It can be used to protect sensitive data when access to
the machine via OS 9 is a concern, for example. However, it also means extra
work encrypting and decrypting all files in the directory, whether or not they
require encryption.

   a. Do not enable File Vault. Users who need to protect files with encryption
are probably better served by creating a disk image with the Disk Utility
program and choosing the encryption option. Only files requiring
encryption will be saved by mounting the disk image and saving them there.

25.4 Use PASSWRD WEB password for the File Vault password – Attributes 2, 3, and
5 –

If File Vault is used (see above), it requires a machine’s administrator to set a
special "emergency" password that the administrator must enter later if a user
has forgotten their password, and needs the File Vault-encrypted data. This is a
risky case of a rarely used password having to be created and then possibly
remembered months or even years later with no use in the meantime.

   a. Use the PASSWRD WEB password protection system to set and protect
the File Vault master password. This will synchronize the File Vault
password with the system administrator password and allow anyone
serving as an administrator to be able to help a user locked out by failing
to remember his/her account password.

25.5 Energy Saver: Never put the computer to sleep – Attributes 2, 3, 5, and 6 –

   a. For desktop systems or portables connected to an AC adaptor, the
energy saver setting shall be set to “never put the system to sleep.”
Some utilities, such as backup operations like TSM, will not function
unless the system is awake. This setting is found in the Energy Saver
system preference.

   /Library/Preferences/SystemConfiguration/com.apple.PowerManagement.plist

25.6 Energy Saver: Put the display to sleep after 30 minutes – Attributes 2, 3, 5, and
6 –

   a. Unless desired by the user, the display shall be set to sleep after 30
minutes of inactivity. Studies have shown that enabling this option can
provide significant cost savings on campus energy requirements. This
setting is found in the Energy Saver system preference.

   /Library/Preferences/SystemConfiguration/com.apple.PowerManagement.plist
25.7 Show warning before emptying the trash – Attributes 2, 3, and 6 –
   a. By default, the Finder will prompt for confirmation when the user chooses
      the Empty Trash command from the Finder menu. This helps reduce the
      likelihood of inadvertently deleting files. Again, this is the OS X default,
      so the Best Practice is to do nothing to change that.

~/Library/Preferences/com.apple.finder.plist

25.8 Set the SNTP to sync to network time – Attributes 2, 3, 4, and 5 –

26.0 Troubleshooting

Some changes to Macintosh computers are useful for troubleshooting, but do not
improve the client experience, efficiency, or system stability. They can help a
computer support professional solve common problems, or eliminate variables in
a troubleshooting session. A troubleshooting tool will incorporate these settings,
automatically changing them to appropriate values whether or not they have
caused or contributed to a problem. The following items shall be used by support
personnel to eliminating problems.

26.1 Delete temporary files in /tmp/###

Some applications create temporary work files in a system directory called tmp,
in a subdirectory named for the user number (commonly 501). A temporary file
that is corrupted can lead to peculiar problems with the application. A good
troubleshooting step is to delete all such temporary files.

26.2 Reset the MacLeland and MacAFS settings to defaults

Some problems with MacLeland and MacAFS can be resolved by resetting them
back to their “factory settings.”

26.3 Reset the computer time to network time

MacLeland, can return unhelpful error messages if the Mac’s clock does not
match the clock on the Kerberos server. resetting the time to a network
standard is a standard troubleshooting step for MacLeland problems. It can be
done through the Date and Time pane of the System Preferences application in
Macintosh OS X.
# Stanford University Web Favorites

<table>
<thead>
<tr>
<th>Ref #</th>
<th>Favorite</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Campus Maps</td>
<td><a href="http://campus-map.stanford.edu">http://campus-map.stanford.edu</a></td>
</tr>
<tr>
<td>10.</td>
<td>Staff</td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>Stanford You</td>
<td><a href="https://stanfordyou.stanford.edu">https://stanfordyou.stanford.edu</a></td>
</tr>
</tbody>
</table>

*Table 6 Stanford University Web Favorites*