Procedures for Updating a Standalone or Private Network Workstation

1. Configure a firewall facing the public network that allows no unsolicited inbound connections and provides DHCP connections to a non-routable private network.

<table>
<thead>
<tr>
<th>Sample Firewall and Client Settings:</th>
<th>Firewall (WAN)</th>
<th>Firewall (LAN)</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>DHCP</td>
<td>192.168.99.1</td>
<td>192.168.99.150</td>
</tr>
<tr>
<td>Mask</td>
<td>DHCP</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>DHCP</td>
<td>**</td>
<td>192.168.99.1</td>
</tr>
<tr>
<td>DNS</td>
<td>DHCP</td>
<td>192.168.99.1</td>
<td>192.168.99.1</td>
</tr>
</tbody>
</table>

2. Create a local administrative account on the workstation. This ensures that the person doing the updates will not have access to sensitive data that might be stored locally in an EFS-enabled directory.

3. Log off the workstation account that is normally used for restricted data work and log in to the administrative account referred to in step 2.

4. Connect the machine being updated to the firewall; reset the NIC as necessary to effect the connection.

5. Initiate the update process
   a. Anti-virus/anti-malware software
   b. Operating system
   c. Appliance software (e.g., Microsoft Office)
   d. Other software (Adobe, etc.)
   e. Add new software products as necessary
   f. Reboot as necessary

6. When updates are complete:
   a. Reboot updated computer
   b. Disconnect the client from the firewall
   c. Log in as local administrator
   d. Reset the NIC (if necessary)
   e. Log out
   f. Log in as secure data user
Procedures for Updating Private Network Workstations

1. Configure a firewall facing the public network that allows no unsolicited inbound connections and provides DHCP connections to a non-routable private network. This device should have a LAN-side static IP which will be used as a temporary gateway value (e.g., 192.168.99.1) by all the private network workstations that are to be updated. It should be connected to the internet before you begin the update process.

2. Each workstation to be updated should be configured to reference the gateway value:
   - Network and Sharing Center >
     - Change adapter settings >
     - (right click) Network Connection.

   This brings up the Local Area Connection Properties box; highlight Internet Protocol Version 4 and select Properties.

   **Sample Firewall, Domain Server and Client Settings:**

<table>
<thead>
<tr>
<th></th>
<th>Firewall (WAN)</th>
<th>Firewall (LAN)</th>
<th>Domain Server</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>DHCP</td>
<td>192.168.99.1</td>
<td>192.168.99.100</td>
<td>192.168.99.150</td>
</tr>
<tr>
<td>Mask</td>
<td>DHCP</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>DHCP</td>
<td>**</td>
<td>192.168.99.1</td>
<td>192.168.99.1</td>
</tr>
</tbody>
</table>

3. Log in at each workstation to be updated using a local administrator account (or domain administrator login). Note: The person doing the updates does not need access to restricted data storage areas.

4. Initiate the update process for each workstation
   a. Operating system updates, validation, etc.
   b. Anti-virus/anti-malware software
   c. Appliance software (e.g., Microsoft Office)
   d. Other software (Adobe, etc.)
   e. Add new software products as necessary
   f. Reboot

5. When workstation updates are complete, disconnect the firewall from its Internet connection.