SMHS Computer Workstation Policies (rev.6/12/17)

The Computer Application Support Services office (CASS) recognizes the importance of properly functioning computer equipment. To that end, we have developed a set of guidelines and policies to minimize computer downtime across the enterprise network.

**CASS Approval of Computer and Other Network Devices**

Any device that will be attached to the enterprise network must be approved by CASS. Failure to obtain CASS approval will result in the device being barred from the network and CASS will refuse to service the device.

Currently, CASS maintains the following hardware specifications for computer support:

<table>
<thead>
<tr>
<th></th>
<th>Dell</th>
<th>Apple</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop</td>
<td>Optiplex All in One</td>
<td>iMAC</td>
</tr>
<tr>
<td>Laptop</td>
<td>Latitude</td>
<td>MacBook Pro</td>
</tr>
</tbody>
</table>

Current lists of detailed standard configurations for Dell Optiplex machines are available from CASS upon request. These standard configurations change frequently, so do not rely upon printed material for the most up to date information.

Network printers are also subject to approval from CASS.

The CASS Assessment form (required for all network-connected devices), is available at [CASS New Workstation Request form](#).

**Data Storage**

In addition to the local hard drive, usually c:, computers on the enterprise network have access to network storage drives. All users have a private Google Drive with unlimited storage. And most users have one or more shared departmental drives. All network drives are backed up nightly. CASS strongly discourages users from storing critical data on the local hard drives because those drives are not backed up. Should a hard drive fail, all data contained on the drive will be lost and will be unrecoverable.

Network drive space is limited and should not be abused. Please perform routine maintenance on your network data files to remove obsolete, irrelevant, or duplicated materials.

**Operating Systems**

CASS supports the following operating systems: Microsoft Windows 7 Professional or newer, and Macintosh OS X 10.10.5 or newer. CASS does not support and will not allow users to operate any Windows Server or any other server OS on the enterprise network. This policy includes the use of server components on approved operating systems: Webservers, FTP servers, game servers, etc., are all
forbidden. If we discover any of these services operating, we will shut down the offending machine and contact GWU Network Security immediately.

**Standard Software Installation**

When CASS performs a computer rollout, we install the following standard applications:

**PC Baseline Rollout**

- Windows 10 64 bit OS
- Microsoft Office 2016 Professional (Word, Excel, PowerPoint)
- Adobe Acrobat X Professional
- Enterprise Virtual Applications
- Google Chrome Web Browser

**Macintosh Baseline Rollout**

- Mac OS X version 10.10.5
- Microsoft Office 2010

**Non-Standard Software Installation**

All software installed on SMHS machines must be licensed. Unlicensed software will be removed.

Because some users require specialized software or have specialized equipment that requires additional software, CASS recognizes the need to deviate from the standard rollout under special circumstances. CASS will install on-standard software only based upon a demonstrated occupational need for the software. Since there are non-standard applications, GW SMHS might not have a site license for the material and it must be purchased by the user or the department.

CASS will not install or troubleshoot non-standard software that does not have a demonstrated occupational need.

Windows operating systems contain powerful components that are not installed as part of a standard rollout. These additional components open vulnerabilities to hackers and represent substantial security risks. Installation of additional windows components, including but not limited to IIS or ICS, is forbidden unless there is a demonstrated occupational need to use these services and prior approval in writing from CASS. If we discover any services which we deem to be security risks operating, we will shut down the offending machine and contact GWU Network Security immediately.

For further information on this policy, please see [User Code of Conduct](#).