Computing Recommendations for Faculty and Staff

The University Technology Council (UTC), in partnership with Information Technology Services (ITS), annually publishes computing hardware and software recommendations for faculty and staff**.** These recommendations reflect institutional and industry trends but do not necessarily take into account the computing requirements of specific Schools or departments. It is highly encouraged that you consult with your local IT staff to purchase a solution that is best for you. These specifications will be updated annually.

The chart below provides recommendations for computer users who require high, medium, or low functionality. The following are definitions of the three categories.

- High: High-end data processing and memory requirements
- Medium: Mid-range data processing and locally-installed desktop applications
- Low: Basic Internet access and low-end applications, such as Microsoft Office

In all cases, warranty and hardware lifecycle of three to five years is recommended.

Hardware Recommendations for New Purchases

For **Desktops**, we recommend any from the Optiplex series.
For **Laptops**, we recommend any from the Latitude series.

Computer Component	**High**	**Medium**	**Low**
Processor	Intel Core i7 or AMD equivalent	Intel Core i5 or AMD equivalent	Intel Core i3/m or AMD equivalent
Memory	16 gigabyte (GB) with expansion space for up to 32 GB or greater	8 GB with expansion space for up to 16 GB	4 GB
Hard Drive	1 TB (7200 RPM) or 256 GB SSD or greater	500 GB (7200 RPM) or 256 GB SSD	500 GB or 128 GB SSD

Laptop Security

In order to ensure the integrity of university data, USC requires all laptops and mobile storage devices that are paid for with university funds and/or used for USC business purposes to be encrypted. As an additional security measure, we strongly encourage that users avoid storing any sensitive data on such equipment altogether. Laptops and mobile storage devices must be either a) delivered with built-in encryption (preferred) or b) accompanied by a software-based encryption solution for subsequent installation. All encryption solutions purchased separately must be installed before the instrument may be used to store or access university data.

This policy applies to laptops and mobile storage devices purchased from all sources of university funds, including sponsored project accounts, and applies to laptops and mobile storage devices used for business purposes but purchased with personal funds.

Windows laptops will require a Trusted Platform Module (TPM) chip to be able to use Bitlocker full disk encryption. Laptops with Mac OS X should use FileVault full disk encryption. Should you have any questions or concerns, please consult your local IT staff for assistance.

Software Recommendations

UTC and ITS recommends all software to be no more than two versions older than the most current version available, and that no end of life (EOL) products be used.

Function	**Software**	**Supported Versions**
Antivirus	Sophos Endpoint Security (REQUIRED)	For Windows and Mac OS 10.x or newest available at http://software.usc.edu
Browser	Individual applications may have specific browser version requirements. For information on the most current browser version available, go to:	
	Apple Safari	www.apple.com/safari/
	Google Chrome	www.google.com/intl/en/chrome/browser/
	Mozilla Firefox	www.mozilla.org/en-US/firefox/new/
	MS Internet Explorer / Edge	windows.microsoft.com/en-us/internet-explorer/download-ie

ITS distributes a variety of software for operating systems free to USC faculty and staff. For more information, please click on the links below. A valid USC login is required.

- **Microsoft Office 365:** https://itservices.usc.edu/office365/
- **Microsoft Office 2016:** https://itservices.usc.edu/officefacstaff/
- **Google Apps @ USC:** https://itservices.usc.edu/googlefacstaff/

Mobile Devices

Mobile devices are defined as tablets and phones that are running a *mobile* operating system such as Apple iOS, Google Android, or Windows Mobile.

Devices paid for with university funds are managed and supported by its local IT departments. Please consult your local IT staff if you have any questions or require assistance.

For mobile devices that were purchased with personal funds, ITS and local IT staff will only provide support to assist its users with accessing USC's network resources, such as USC Wireless and email. Documentation on accessing these resources can also be found through http://ITServices.usc.edu.

We recommend all users keep their mobile devices secure by following basic best security practices, such as activating screen lock, enable remote wipe/lock feature (if available) and backing up data regularly. *Note: UTC and ITS recommends all software to be no more than two versions older than the most current version available, and that no end of life (EOL) products be used.*

Purchasing Hardware through Business Services-Procurement

Business Services-Procurement has worked with our suppliers to negotiate pricing on laptops and desktops that meet or exceed these standards above. It is recommended that you consult with your local IT staff to purchase a solution that is best for you.

Data Security

All USC faculty, staff and students are required to comply with the University's Network Infrastructure Use Policy and its stated requirements for the protection of sensitive data. For more information, see the USC Network Infrastructure Use Policy. http://policy.usc.edu/network-infrastructure/

eWaste

Whenever possible, choose the environment and select green products. It is recommended that you consult with your local IT staff to assist in the disposal of electronic waste responsibly and securely. For more information on eWaste, see the USC Sustainability department's Electronic Waste page. http://green.usc.edu/content/electronic-waste