Columbia Business School
AT THE VERY CENTER OF BUSINESS™

Supported Computer Configuration Policy

Revised January 26, 2017

1. Scope

Computers and related devices owned by the Columbia University Business School ("CBS").

2. Governing Policies

a. Columbia University's Registration and Protection Endpoints Policy: III.B.1-5, 6 and 7[1]
b. CBS's Faculty Expense Policies for Business School, section 8 bullet one, section 9 bullets one and two, and Section 5 bullet two
c. CBS's Desktop Backup and Collaboration Tools, sections 5 and 6

3. Summary

All CBS owned computers must meet specific minimum operating system and software configuration requirements to be eligible for ITG support and CBS network access.

The intent of this policy is to create a secure, functional, manageable and useful computing environment for all CBS constituencies.

In most cases, ITG will provide these elements to the client when the computer is purchased as a standard configuration package (a.k.a. "image"). During the asset's lifecycle, in the event of a computer virus or other technical issue which compromises the integrity or usability of the computer, ITG may at its discretion and in consultation with the client, wipe the computer and re-apply this standard configuration (a.k.a. "re-image").

4. Policy Details

CBS supported assets will have an ITG asset tag affixed to them and will conform to the following items as outlined in the table below:

		Microsoft Windows	**Apple Mac**
a.	Supported Operating System[2]	Windows 7 Professional or Enterprise Windows 10 Enterprise	OSX 10.10 (Yosemite) OSX 10.11 (El Capitan) macOS 10.12 (Sierra)
b.	Required Operating System Updates	Windows Update Server (WSUS) managed centrally	Apple App Store managed locally
c.	Configuration Management	Service Center Configuration Manager (SCCM) Active Directory	Casper Active Directory
d.	Anti-Virus & Malware Protection	Sophos	Sophos

[1] Since some computers cannot always be physically protected (i.e. loss during travel), CBS meets the section III.B.7 requirement for laptops through physical disk encryption.

[2] In exceptional cases when required for faculty research, Linux may also be supported as an operating system on a best effort basis.

e.	Full-disk encryption[3]	BitLocker	FileVault
f.	Data Backup & Recovery	CrashPlan	CrashPlan
g.	Inventory Management	via WMI	via SSH

5. Policy Exceptions (faculty only)

Exceptions to specific aspects of this policy may be granted to faculty by CBS's Chief Information Officer. The allowable exceptions and related caveats are listed below:

a. **Encryption -** By opting out of BitLocker or FileVault, the client takes full responsibility for protecting their data themselves and agrees that their COSTAR (and no other CBS funds) will pay for any required services in the event of a loss.
    i. Generally, there should not be any performance difference with encryption enabled unless running large statistical analyses, which themselves are best run on the Research Grid. However, should large jobs need to run locally where encryption would create a noticeable performance impact, an exception may be granted.
    ii. Any computers with sensitive or confidential data are not eligible for an exception and are subject to sections III.E and III.F of the referenced University policy.

b. **Backup & Recovery -** By opting out of CrashPlan, the client takes full responsibility themselves and agrees that their COSTAR (and no other CBS funds) will pay for data recovery services in the event of a loss.

c. Anti-Virus & Malware Protection – The client may opt to utilize the anti-virus tool provided by the Columbia University Information Technology department ("CUIT") in lieu of the anti-virus tool provided by CBS.
    i. Should the computer become compromised in any way, ITG's only remediation will be to ensure data has been backed up, and then re-image the machine as referenced in Section 3 above.

d. **Required Operating System Updates –** In extremely rare cases where running Windows Updates could damage an ongoing research project, a computer may be removed from the automated Windows Update services server (currently WSUS).
    i. The client takes responsibility for all security patching on this computer, and the computer may be subject to random audits and loss of network access in the event a security risk is introduced.

[3] All laptops and only desktops with sensitive data/access.