B) Resources for those who self-support a Cornell-owned computer

This page includes a resources table compiled by Chemistry IT

See also

- Self-support of a Cornell-owned machine
- A) Set-up options for a self-supported Cornell-owned computer
- Chemistry's Computer Exception Form and related networks

Resources table compiled by Chemistry IT

Task or Responsibility	Tips, courtesy ChemIT	FYI: How it is done for managed computers.	Notes
Purchasing	You don't have to purchase what ChemIT recommends or brands we normally buy. If not a ChemIT-specified system, the actual purchase, per University Purchasing, is by definition an "exception" and must be vetted by the Arts & Sciences' ITSG, Frank Strickland: • https://www.dfa.cornell.edu/procurement/tools-forms/forms/exception-ordering Optional: We are available for consultation as well to facilitate your group buying the right items yourselves. • Values we likely share with your group include lower cost, more effective repair and warranty services, and long-term viability.	We purchase almost all computers in Chemistry, saving researchers thousands of dollars every year, time, and, administrative aggravations.	The fastest, easiest, and cheapest way to buy a computers and related technologies is usually through Chemistry IT.
Hardware inventory	All computers and printers must be noted in ChemIT's inventory, usually with assistance of the group's IT Rep. • Please notify your IT Rep. if the computer changes location so they can inform ChemIT- thank you.	ChemIT is responsible for inventorying all Cornell computers in Chemistry.	
Creating an Admin account	Creating a strong password is required by Cornell policy. More security tips: • http://www.it.cornell.edu/security/how.cfm?cat=4&tip=144	Group's faculty member and group's IT Rep. is offered this account, using password entered by IT Rep.	Cornell Policy 5.4.1, p9: Protect the resources under your control with the responsible use of secure passwords and by appropriately establishing an administrator password. • https://www.dfa.cornell.edu/sites/default/files/vol5_4_1.pdf http://www.it.cornell.edu/security/how.cfm?cat=4
Creating and primarily using a User (non-Admin) account	This practice is required by Cornell policy	Automatic, via Cornell's Active Directory	Cornell Policy 5.10, p16: Configure user privileges to be as low as possible while still meeting operational needs. Consistent or regular use of any account with administrative privileges is inappropriate. • https://www.dfa.cornell.edu/sites/default/files/vol5_10.pdf
Backups and restores.	• Ensure user keeps critical files on group's file share or other off-device location. • User can have group pay for EZ-Backup and ChemIT can assist administratively.	Encourage use of group's file share so no back-ups required to be set up, monitored, and paid for on the computer itself. Critical systems get set up with EZ-Backup.	Hard drives, even solid state ones, do fail. People make mistakes. Bad luck happens. Plan ahead! • Backup ideas for personal computers • http://www.it.cornell.edu/services/ezbackup/

Keeping the operating system (OS) and applications versions current and patched.	Patch within 14 days, as required by Cornell policy. From IT Security Office: University Policy requires computers connecting to the Cornell network to be updated and patched against viruses and malware. Since no more updates and patches will be available for older unsupported operating systems to meet new threats, these older computers that connects to campus network resources will effectively be non-compliant with University Policy.	We upgrade via active migration to keep on current OS.	Cornell Policy 5.10, p16: Keep all relevant operating system, server, and application software up-to-date (patched). Develop and document a patch management process such that all vendor defined security or critical software updates are installed as soon as possible, but no later than 14 days after their release. • https://www.dfa.cornell.edu/sites/default/files/vol5_10.pdf
Anti-virus	Windows: Use built-in MS anti-virus and keep it updated. Mac: Use MS SCEP and keep it updated. Obtain installer from ChemIT.	Windows: Managed anti-virus (MS SCEP) Mac: Unmanaged anti-virus (MS SCEP)	Cornell Policy 5.10, p17: On all Windows and Macintosh systems, run anti-malware (anti-virus, etc.) software with daily updates and active protection enabled. • https://www.dfa.cornell.edu/sites/default/files/vol5_10.pdf
Responding to IT Security Office inquiries	If system compromised, you must work with IT Security for clean-up and for the system be be allowed back on the network.		
Installing local printers	Use group printer's DNS name: • https://confluence.cornell.edu/x/LAkkD	ChemIT installs.	
Installing MS Office	Download from Office 365 account (up to 5 installations) • http://www.it.cornell.edu/services/office365/apps/student.cfm • http://www.it.cornell.edu/services/office365/apps/faculty-staff.cfm	Use Cornell's central licensing infrastructure and processes for IT support providers for unlimited installations.	Macs: Know what versions of Office work better with ChemDraw: • ChemDraw and Office 2016 on Macs
Adobe applications (Acrobat, Photoshop and other components of the Adobe CS suite)	Obtain ChemIT's services for them to install, with your Admin credentials, required applications using Cornell's site license.	Use Cornell's central licensing infrastructure and processes for IT support providers for unlimited installations.	CIT's licensing info: • http://www.it.cornell.edu/services/software_licensing/available/Adobe-Creative-Cloud-Enterprise-Licensing.cfm#acrobat • http://www.it.cornell.edu/services/software_licensing/available/Adobe-Creative-Cloud-Enterprise-Licensing.cfm#cc
ChemDraw	Download from CambridgeSoft, using Cornell license: • http://blogs.cornell.edu/chemit/chemdraw/	ChemIT installs.	
Encryption: Whole-disk	Implement and escrow keys. • http://www.it.cornell.edu/security/how.cfm?cat=6&tip=146 Required by Cornell policy, with a grace period until January 2017 (as of April 2016).	Planning underway (as of April 2016). Will use Cornell's key escrow service built into MBAM, for IT Support Providers.	By Jan 2017: Cornell Policy 5.10, p17: All university-owned desktops, laptops, smartphones, tablets, and other portable computing devices must utilize whole-disk-encryption software to protect all local, persistent storage when the system is powered off.