Computer Acceptable Use Policy

In order to maintain a secure and supportable computing environment for the faculty, staff, and students of Chemistry and Biochemistry and Molecular Biology, we have established the following policies regarding acceptable computer use for all members of these departments.

Getting Help If you have information technology (IT) issues or questions, please send an email to either:

ithelp@biochem.umass.edu
or
ithelp@chem.umass.edu

In an emergency, or if sending email is not possible, please call: John Maher (413-577-3120), Sam DeLaughter (413-545-6085), or Gary Rehorka (413-577-3150)

NOTE: The University Acceptable Use Policy (AUP) applies to the entire campus. By accepting the BMB/Chemistry AUP you also agree to abide by the University of Massachusetts/Amherst AUP (http://www.it.umass.edu/security/acceptable-use-policy).

Policies

The following is not a comprehensive list of requirements. Any activity that adversely affects the functioning of IT resources in the Departments is prohibited.

1. Your computer must be up-to-date with security patches.
2. Your computer must have up-to-date anti-virus software and must be scanned regularly for potential problems.
3. You must use only those computing and information technology resources for which you have authorization.
4. Your LDAP password should not be given out to other people, sent over email, or written down in obvious places.
5. You must ensure that sensitive data are created, collected, maintained, used, disseminated, and destroyed in a manner that prevents unauthorized use, corruption, disclosure, loss or theft. (If you need help installing and using encryption software, contact the BMB/Chemistry IT team.)
6. If your computer was purchased with University funds, you must use whole disk encryption on that computer.
7. Abide by applicable laws and university policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.
8. Any system that is intended to be run as a server needs to be discussed with the IT staff prior to deployment.
9. Running a network analysis or testing tool (e.g., port scanning software) is prohibited unless cleared in advance by IT staff.
10. Any suspected compromise or infection of a system must be brought to the immediate attention of IT staff.
11. All network activity must not adversely impact the proper function of the network.

Links regarding sensitive data and anti-virus software:
http://www.it.umass.edu/support/security/data-classification-umass-amherst
http://www.it.umass.edu/support/security/university-data-commercial-storage-collaborative-services-umass-amherst
http://www.it.umass.edu/software/mcafee-virusscan-enterprise

If you have any questions or need assistance with any of the above items, please contact us via one of the helpdesk email addresses: ithelp@biochem.umass.edu or ithelp@chem.umass.edu