

An Easy Guide to the Appropriate Use Policy at the University of Illinois at Urbana-Champaign

Any University policy can be tricky to navigate, especially for new hires at the University. This guide will help you understand the Policy on Appropriate Use of Computers and Network Systems, which is often referred to as the AUP. For the average member of the University of Illinois community, Section 4 of the AUP, “Proper and Authorized Use of UIUCnet” is what they need to understand. This guide will explain quote and then explain the most important parts of Section 4. However you should still take time to read the entire AUP as following it is an expectation of employment. The AUP can be found online at: <http://www.cio.uiuc.edu/policies/>

Section 4 - Proper and Authorized Use of UIUCnet

“While CITES does not routinely monitor appropriate use of UIUCnet by individuals, the CITES Security Office will respond to complaints or other notifications of inappropriate use.”

What It Means: CITES is not watching your every click at your computer. Network traffic is not examined except in the case of a security incident.

“Use of UIUCnet is a privilege, not a right, and such use may be suspended or terminated at the direction of the CITES Security Office when, in its judgment, this policy has been violated by the user.”

What It Means: If you improperly use your computer, or if your machine becomes compromised, you could lose access to the network and the internet.

Section 4(a) - Purpose of UIUCnet

“UIUCnet exists to support the educational, research, and public service missions of the University, and its use should be limited to those purposes.”

What It Means: You should use your computer and UIUCnet for work related activities, not for eBay, watching movies, or other personal uses.

Section 4(c) - Appropriate Use of UIUCnet

“No individual may use UIUCnet resources for commercial or profit-making purposes or other purposes that interfere with the mission of the University.”

What It Means: Don't use your machine for your home business, political campaigning, freelancing, or even for eBay.

“As with all University computing and network facilities, UIUCnet may not be used for improper or illegal purposes, such as unauthorized use of licensed software, intentional efforts to breach security, or the transmission of computer viruses.”

What It Means: Do not pirate software, music or movies on your University computer. Do not attack the University IT resources. Do not let your machine become infected with viruses or bots that could cause problems without you even knowing.

Section 4(c)(ii) - Responsibility to maintain privacy of passwords

“Passwords associated with an individual’s network IDs and computer sign-ons should not be shared without authorization. Compromised passwords may affect not only the individual, but also other users on campus or on the Internet.”

What It Means: It is vital that you set a strong password, and that you do not share it with anyone. Also, never write down or email your passwords.

Section 4(c)(iv) - Appropriate Use of Bandwidth

“As described in Section 10 below, bandwidth both within campus and connecting to the Internet is a shared, finite resource. Users of UIUCnet must make reasonable efforts to use this resource in ways that do not negatively affect others.”

What It Means: You should try to avoid programs that hog bandwidth, such as file sharing programs and Skype. If you must use one of these programs, configure it to minimize its impact on the campus network.

Section 4(d)(i) - Passwords and University Units

“Faculty and staff, including student employees, must not under most circumstances share their passwords with others, even with supervisors.”

What It Means: Never email anyone your password. Never write down your password. Never tell anyone your password. There will never be a time where supervisors or your IT staff will ask for your password.

Section 4(d)(ii) - Use Unrelated to University Positions

“Use by University employees unrelated to their University positions must be limited in both time and resources and must not interfere in any way with University functions or the employee’s duties. It is the responsibility of employees to consult their supervisors, if they have any questions in this respect.”

What It Means: In most cases, it is not a problem to take a few minutes to check your personal email, or other to do other trivial personal tasks. However, it is best to discuss with your supervisor what is an acceptable amount of personal usage of University resources.

If you have further questions about the Appropriate Use Policy, or other basic security and policy questions, please contact CITES Security at securitysupport@uiuc.edu