



CSEE Computing Lab Policies

Access to the Department of Civil, Structural, and Environmental Engineering (CSEE) computing labs is a privilege provided to undergraduate and graduate students in CIE/ENV majors. Lab facilities are to be used for academic work only; personal use is prohibited and could result in loss of access.

All students are required to follow the UB Information Technology (UBIT) policies for computing lab use, which are maintained at:

<http://www.buffalo.edu/ubit/policies/it-policies-a-to-z/computer-and-network-use.html>

In addition to the UB-CIT policies, the following rules apply to the CSEE labs:

1. Only CIE/ENV majors are to use the computers in the CSEE Computing Labs (CIE/ENV majors are automatically registered).
2. The CSEE computers are for academic use only. Approval is required for research usage. Downloading of files for personal use, or saving files to local hard drives is strictly prohibited, and could result in loss of access.
3. **THE DOORS TO THE LAB MUST BE CLOSED AT ALL TIMES; PROPPING OPEN THE DOORS IS PROHIBITED.**
4. You may bring covered drinks into the lab, however, food is not allowed.
5. One user per computer. User must log in using UBIT login, must remain with the computer while it is in use, and must log off when session is complete.
6. Unattended processes are subject to termination by the system administrator.
7. All work should be saved to a portable storage device.
8. Computers are to be left on at all times. Shutting down computers is prohibited. After logging off, any hardware problems should be reported by sending an email to Science and Engineering Node Services (SENS) at senshelp@buffalo.edu
9. Students may not move supporting hardware, including but not limited to teaching station(s), networking cables/switches, and/or security cameras.

Violation of these policies will result in temporary or permanent loss of lab privileges at the discretion of the CSEE Department Chair, in conjunction with other penalties as defined in the UBIT policy. CSEE and SENS reserves the right, upon reasonable cause for suspicion, to access all aspects of its computing systems and networks, including individual login sessions to determine if a user is violating this policy or state or federal laws.