



ESM Department Network and Computer Policy —ESMIT10

www.esm.psu.edu/policies/network

This policy is for all Penn State Engineering Science and Mechanics students, faculty, staff, visitors and others requesting access to the department's computer network.

Users of computers or other devices connected to the university network must agree to the following:

- *University Policy AD20, AD23, AD54 and the College of Engineering Computing Policies.*
- *Run only legal and certified Operating Systems and software.*

Only OS 10.2 or higher for Apple based systems may be installed, and only Windows 2000 Professional or XP Professional for PCs. All other installed software must be legally licensed for the machine or user. Material that infringes on copyrights may not be stored or accessed on any machine.

- *Must not run server or hosting software of any kind.*

This includes file sharing applications such as eMule, BitTorrent or Gnutella clients like BearShare or LimeWire. Services such as Web servers, FTP services, SMTP, TelNet etc. are prohibited. Central server storage is available at the request of your advisor. Port scanning is strictly prohibited.

- *Participation in the College of Engineering Active Directory (domain) where applicable.*

The College of Engineering (COE) Domain offers additional security features to which all PC users are required to attach: a user account is not required. Machines may be exempted only with express, written approval of IT Staff and Department Head (See Form ESMIT08).

- *Must have secure login, and must not have multiple users share a single account.*

All computers must have uniquely identifiable access (i.e. separate accounts) for all users. Machines must present a login screen for secured login and must not automatically log a user in. Guest and other non-secure accounts must be disabled or deleted. Sharing of passwords and user accounts is strictly prohibited, and new accounts must be authorized by appropriate faculty and IT staff. This form authorizes only the listed user to access network resources.

Continued on other side ...

- ***Reasonably complex passwords: logging turned on.***

All login passwords must meet COE Password Complexity Rules below, and Login and System event logging must be turned on and produced on demand.

The College of Engineering requires that you change your access password at least once every 6 months. This may seem bothersome at first, but it really is one of the best methods to ensure that your password remains secure. It is mandatory to create a password that follows these criteria:

- A password must contain at least 6 characters.
- A password must contain at least 3 of the 4 types of characters (upper-case, lower-case, numbers, and punctuation).
- A new password must not match your last 5 passwords.
- A password must not contain your first name, last name, or user ID.
- Installation of all security patches.

Security notices may be sent to ESM faculty, staff and students from time to time. It is incumbent upon the user to install these and other security patches in a timely manner. Updates should be checked regularly with Software Update (Macs) or Windows Update (PCs). ** all Windows machines must have the latest Service Pack installed and be secured before connecting to the network for the first time **

- ***Anti-virus software installed, maintained and active.***

Users are required to make an effort in good faith to protect against the spread of internet worms and viruses. Active protection is required as well as daily scans. Please note that the university is licensed for Symantec Anti Virus which can be downloaded and installed directly from <https://downloads.its.psu.edu>

- ***Allow security scans by authorized university personnel.***

University Policy requires department, college and university security staff to regularly scan assigned network space for possible infections, vulnerabilities or compromised systems. Any efforts to circumvent or block these scans will result in immediate suspension of network privileges.

- ***Report changes or updates of requested machine or user immediately to ESM IT Staff.***

Network access via assignment of an IP address is only permitted for the given user and machine in the listed state or configuration on this form. Any changes must be reflected in a new ESMIT06 application.

Failure to comply with university, college or department computing policies may result in loss of network access privileges, loss of university 'access' account, or confiscation of equipment. ESM IT staff have the right to filter, quarantine or restrict any computing device from the ESM network at any time.

Return this form to the mailbox of Craig Haynal or William Ames in 212 EES Bldg.

For assistance please contact the ESM IT staff at accounts@email.esm.psu.edu or by calling 863-6029.

This policy is subject to change without notice. Check www.esm.psu.edu/policies/network for current policy.

Signature

Date

PSU ID Number