

Printed Name: _____

PSU Access Account : _____

User Acknowledgement Form

You have been given access to network and computing resources provided by the College of Earth and Mineral Sciences. This computing infrastructure includes Windows Active Directory services, electronic mail, and disk storage and is intended to support the College's day to day Information Technology needs.

Use of the IT infrastructure for other purposes is prohibited without the prior approval of the IT group. The IT group reserves the right to limit or suspend your account without prior notice if your use adversely impacts the operation of the College's computer systems or networks.

The College's computing environment contains a number of licensed software packages. When using licensed software, you are responsible for proper use of all software and for compliance with commercial licensing agreements negotiated by the University. This includes careful review of and compliance with all restrictions. You may not copy licensed software installed on the College servers to other systems, or install software onto College systems without permission from the IT staff.

All passwords for newly activated user ids must be changed when first used. The EMS IT support group can assist you with this procedure. Thereafter, the system will require users to change their password every 12 months.

A password is private information. All use of the user id is assumed to be performed by the person assigned to that user id. You are responsible for safeguarding the password for your user id. Password sharing is prohibited by University Policy and both State and Federal law.

The following password guidelines are based upon experience and common sense. Your password:

1. Must be at least eight characters in length and be resistant to password cracking programs.
2. Must not include a word that may be found in a dictionary.
3. Should not be information easily obtainable about you. This includes your license plate number, social security number, telephone numbers, or street addresses.
4. Must not be the same as your user id.
5. Must not start with or end with your initials.
6. Must not include your first, middle, or last name.
7. Must contain a mix of characters from three of the following four groups: lowercase characters (a-z), uppercase characters (A-Z), numbers (0-9) and special characters (@, !, #, \$, %, ^, etc.)

Rooms containing computers connected to the College network must be secured when unoccupied.

Printed Name: _____

PSU Access Account : _____

Please remember, it is your responsibility to properly handle and store any data considered "sensitive" by the University, State, or Federal law. Data that falls into this category is covered by University Policy AD-23 and includes, but is not limited to: HR, financial and student records (including grades), Social Security numbers, medical data, "human subject" research data and other "personally identifiable information".

The College's backup and disaster recovery procedures make a copy of all data stored on its servers along with selected data directories on workstations supported by the College IT group. These backups are kept for up to 2 months before they are destroyed. The backup system is run in a manner that is considered secure for all types of "sensitive data". More information on backups and recovery can be found on the EMS IT support site referenced at the end of this document.

Computer abuse and network security are significant problems at Penn State and elsewhere. You are expected to exercise responsible, ethical behavior when using the University's and College's computers, information, networks, and resources. You must comply with all applicable University policies, State, and Federal laws. Copies of University Policies AD-20 (Computer and Network Security), AD-23 (Use of Institutional Data), University Administrative Guidelines ADG-1 (Glossary of Computer Data and System Terminology), and ADG-2 (Computer Facility Security Guideline) are available online at <http://guru.psu.edu/policies/> for your review.

Violation of any provisions of these policies may result in (i) a limitation on a user's access to some or all University systems, (ii) the initiation of legal action by the University against the violator, (iii) the requirement of the violator to provide restitution for any improper use of service, and (iv) disciplinary sanctions, which may include dismissal.

Please confirm that you are aware of the provisions of these policies and guidelines by printing your name and PSU Access Account ID, initialing and dating each page, and signing and dating below.

Signature

Date

Printed name

For assistance, please contact the EMS IT support group:

Web: <http://it.ems.psu.edu/>
Email: helpdesk@ems.psu.edu
Telephone: 814-865-1800
Room: 246 Deike Building