

Eberly College of Science

Acceptable Use Policy

Table of Contents

- 1.0 Purpose
- 2.0 Scope
 - 2.1 People
 - 2.2 Equipment
- 3.0 Policy
 - 3.1 General Use and Ownership
 - 3.2 Roles, Rights and Responsibilities
 - 3.2.1 Users
 - 3.2.2 Administration
 - 3.2.2.1 System Administrators
 - 3.2.2.2 Network Administrators
 - 3.2.2.3 ECOS Administration
 - 3.3 Acceptable Use
 - 3.3.1 Security
 - 3.3.2 Confidential and Proprietary Information
 - 3.3.3 Copyright and Intellectual Property
 - 3.3.4 Illegal Activities
 - 3.3.5 Responsible Use
 - 3.3.6 Reporting Violations and Vulnerabilities
 - 3.4 Privacy
 - 3.5 Exceptions and Exemptions
- 4.0 Enforcement and Penalties
- 5.0 Additional Resources and Information
- 6.0 Revision History

1.0 Purpose

To establish terms, conditions and requirements in regard to the use of computer, network, and other technology resources within the Eberly College of Science (ECOS). The material contained herein is a supplement to Penn State policy AD20. In the event of confusing or conflicting statements, the terms and/or definitions in AD20 should be used.

2.0 Scope

2.1 People

This policy applies to all faculty, staff, students, visitors, guests, contractors, consultants, temporaries, and other workers within ECOS, including all personnel affiliated with third parties.

2.2 Equipment

This policy applies to all desktop & laptop computers, handheld devices, network devices, or any other type of computing or networking equipment that is connected to the ECOS Network.

3.0 Policy

3.1 General Use and Ownership

The ECOS Network is a dynamic environment that provides interactive communication between buildings, people, and devices. The ECOS Network encompasses any and all network structures and/or devices within the College. Any device connected to the ECOS Network, even a personally owned one, becomes subject to the rules and regulations set down by the College. By utilizing the network connectivity available, you are agreeing to abide by ECOS IT policy.

3.2 Roles, Rights and Responsibilities

3.2.1 Users

3.2.1.1 Definition of a User

Any individual who uses ECOS computing and/or network resources.

3.2.1.2 User Rights & Responsibilities

Users may use the computing systems of ECOS in any manner required to properly perform their job provided that such use does not conflict with University or ECOS policy nor disrupt the network in any way.

Users are responsible for ensuring their own data and equipment is in compliance with University and ECOS policy.

3.2.2 Administration

3.2.2.1 System Administrators

ECOS System Administrators manage the shared resources of the department to which they are assigned, including mail, web, login, and other services as required. ECOS System Administrators also build, configure, secure and maintain user workstations for classrooms, labs and end-users.

If you manage your own computer equipment on the ECOS Network you are an ad-hoc System Administrator and as such you are required to know and comply with all ECOS and University policies for all devices you maintain.

3.2.2.2 Network Administrators

ECOS Network Administrators manage the physical and logical aspects of network connectivity within the College, including routers, switches, hubs, firewalls, wireless access, physical media and other elements as required.

University policy prohibits the extension of the network beyond officially maintained devices and subnets. Personal routers, switches, hubs and wireless networks are not permitted.

3.2.2.3 ECOS Administration

The administrative offices of ECOS are responsible for defining and enforcing official computer and network policy within the College. Formal requests for change to an existing policy, or disputes over policy violations must be in writing and should be submitted directly to the Associate Dean responsible for overseeing IT Resources within the College. Informal requests for exceptions and exemptions may be submitted electronically to the IT Manager within your department.

3.3 Acceptable Use

3.3.1 Security

3.3.1.1 Access to computing and network devices is given on an individual basis. Sharing of account access is prohibited.

3.3.1.2 Access controls such as passwords, SecureID tags, cryptographic keys and/or other security tokens may not be shared with anyone, including friends, co-workers and family members.

3.3.1.3 All computing and network devices must be secured with a password or other approved authentication method(s).

3.3.1.4 Logging, when available, must be enabled.

3.3.1.5 The University provides antivirus software free of charge. Use of this software is required for devices connected to the ECOS Network.

3.3.1.6 IP addresses must be assigned by IT staff, and may not be arbitrarily taken.

3.3.1.7 Encryption must be used when transferring sensitive or confidential university data over an unsecured network link.

3.3.1.8 Users may not knowingly introduce malicious software such as viruses, Trojans, worms, etc.

3.3.1.9 Users may not willfully circumvent network security measures. This includes unauthorized network and vulnerability scanning.

3.3.2 Confidential and Proprietary Information

3.3.2.1 Users must take appropriate steps to secure any and all data that has been classified as confidential.

3.3.2.2 Sensitive data should be encrypted when possible.

3.3.3 Copyright and Intellectual Property

3.3.3.1 Violations of copyright, software license agreements, control laws, or use of pirated software is prohibited.

3.3.4 Illegal Activities

3.3.4.1 Under no circumstances is a user on the ECOS Network authorized to engage in any activity that is illegal under local, state, federal or international law, or in violation of University policies.

3.3.4.2 The ECOS Network and ECOS-owned equipment may not be used for hosting, promoting, or otherwise assisting any commercial, abusive, obscene, or other activities that may reflect poorly upon the College or the University.

3.3.5 Responsible Use

3.3.5.1 The ECOS Network may not be used to send or relay unsolicited, bulk email (commonly known as 'spam') or newsgroup postings.

3.3.6 Reporting Violations and Vulnerabilities

Violations of ECOS policy should be reported to the IT staff of your department. Each department maintains a "security@" email address for this purpose (example: security@phys.psu.edu).

3.4 Privacy

Users on the ECOS Network shall have a reasonable expectation of privacy. Access to personal and/or private data by System Administrators, Network Administrators or other Users is prohibited unless explicitly authorized under the guidelines set forth in University Policy AD53.

3.5 Exceptions and Exemptions

Departmental IT Managers may approve exceptions and exemptions to ECOS policy as required by the needs of the faculty and staff. All exceptions and exemptions must be documented. Disputes will be resolved by the ECOS administrative office.

4.0 Enforcement and Penalties

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the College, or the University.

5.0 Additional Resources and Information

- PSU IT (AD20): <http://guru.psu.edu/policies/AD20.html>
- PSU Privacy (AD53): <http://guru.psu.edu/policies/AD53.html>
- Glossary: <http://guru.psu.edu/policies/adg01.html>

6.0 Revision History

Revision	Date	Author
1.0	May 25, 2007	Joshua Fritsch (joshua@phys.psu.edu)
2.0	Aug 28, 2007	Joshua Fritsch (joshua@phys.psu.edu)
2.1	Aug 29, 2007	Joshua Fritsch (joshua@phys.psu.edu)
2.2	Aug 30, 2007	Joshua Fritsch (joshua@phys.psu.edu)
2.3	Sep 3, 2007	Joshua Fritsch (joshua@phys.psu.edu)
2.4	Sep 13, 2007	Joshua Fritsch (joshua@phys.psu.edu)
2.4.1	Sep 17, 2007	Joshua Fritsch (joshua@phys.psu.edu)