Policy 901

1 Introduction

1.1 The University provides computer access and capabilities through Information Technology Services and various Colleges and departments. The University relies heavily upon these systems to meet operational, financial, educational and informational needs. It is essential that Appalachian's computer systems, and computer networks, as well as the data they store and process, be operated and maintained in a secure environment and in a responsible manner. It is critical that these systems and machines be protected from misuse and unauthorized access. This policy applies to all University computer systems and refers to all hardware, data, software and communications networks associated with these computers. In particular, this policy covers computers ranging from multi-user timesharing systems to single user personal computers, whether stand-alone or connected to the network. In addition to this computer policy, users of these computer systems are subject to applicable state and federal laws. Computer abuse will be referred to the Chief Information Officer, the Director of Technology Support Services and/or the appropriate person affiliated with a college or department computer facility. Computing resources are valuable, and their abuse can have a far-reaching negative impact. Computer abuse affects everyone who uses computing facilities. The same morality and ethical behavior that applies in the non-computing environment applies in the computing environment.

2 Scope

2.1 Individuals Covered by this Policy

2.1.1 This policy applies to all members of the Appalachian State University community including students, faculty, staff, visitors and contractors of the University.

3 Definitions

3.1 Computer Systems

Computer systems includes any microcomputer (stand-alone or networked), workstation, mini-computer or mainframe computer used on this campus or accessible by way of networks, at other locations.

3.2 Computer Networks

Computer networks includes any local or wide area communications systems connecting computer systems as defined above.

3.3 Local Area Networking Media

Local area networking media may consist of copper wire, fiber optic cable, thin or thick wire cable which is used to connect one terminal, microcomputer, workstation etc. to another or to network interface equipment.

3.4 Internet

A vast international computer network of many component networks. It contains the ability for electronic mail (e-mail), network news, file and image transfer and information browsing.

3.5 World Wide Web (WWW)

The more graphical based component of the internet that encompasses many thousands of text, graphic, audio and video files interlinked throughout the world.

4 Policy and Procedure Statements

4.1 Common Forms of Computer Abuse

4.1.1 Misuse or abuse of computers, computer systems, computer networks or any other electronic communication technologies
is prohibited. The following topics are considered areas of abuse:

1. Privacy vs Open Records. Investigating or reading another user's files is considered the same as reading papers on someone's desk - a violation of their privacy. Reading protected files, by whatever mechanism, is considered the same as "breaking and entering." Violations include, but are not limited to:
   1. attempting to access another user's computer files without permission;
   2. supplying or attempting to supply false or misleading information or identification in order to access another user's account;
   3. deliberate, unauthorized attempts to access or use University computers, computer facilities, networks, systems, programs or data;
   4. the unauthorized manipulation of Appalachian's computer systems, programs or data.
   5. the unauthorized capturing of computer network data directly from network backbone or local area networking media.

2. Use of electronic communication technologies to engage in harassment as defined by Appalachian Policy 110.

3. Theft includes the stealing of any property of the Institution, or State of North Carolina. Violations include, but are not limited to:
   1. using subterfuge to avoid being charged for the use of computer resources;
   2. deliberate, unauthorized use of another user's account to avoid being billed for the computer usage;
   3. abusing specific computer resources, such the INTERNET or the World Wide Web (as described in other publications);
   4. attempting unauthorized access to computers outside the University using the University's computers or communications facilities;
   5. removing any computer equipment (hardware, software, data, etc.) without written authorization;
   6. copying, or attempting to copy, data or software without proper authorization.

4. Vandalism - Any user's account, as well as the operating system itself, is a possible target for vandalism. Attempted or detected alteration of user system software, data or other files, as well as equipment or resources disruption or destruction, is considered vandalism. Violations include, but are not limited to:
   1. sending either mail or a program which will replicate itself or do damage to another user's account;
   2. tampering with or obstructing the operation of the Universities' computer systems (for example, attempting to "crash" the system);
   3. inspecting, modifying, or distributing data or software without proper authorization or attempting to do so;
   4. attempting to interfere with the performance of the system;
   5. damaging computer hardware or software.

5. Unauthorized Business Usage includes any use of university resources for promoting or conducting business for personal use. Violations include, but are not limited to:
   1. sending mass mailings
   2. using computer accounts for work not authorized for that account

6. Copyright Issues - The University owns licenses to a number of proprietary programs. Users who redistribute software from the computing systems break agreements with its software suppliers, as well as applicable federal copyright, patent and trade secret laws. Therefore, the redistribution of any software from computing systems is strictly prohibited except in the case of software which is clearly marked as being in the public domain. Violations include, but are not limited to copying, transmitting, or disclosing data, software or documentation without proper authorization.

7. Miscellaneous - Other uses commonly considered unethical, such as:
   1. unauthorized and time consuming recreational game playing;
   2. using computer accounts for work not authorized for that account;
   3. sending chain letters or unauthorized mass mailings;
   4. using the computer for any illegal purposes;

4.2 Computer Usage Guidelines

1. Users are to have valid, authorized accounts and may only use those computer resources which are specifically authorized. Users may only use their account in accordance with its authorized purpose. Users are responsible for safeguarding their own computer account. Users should not let another person use their account unless authorized by the system administrator for a specific purpose. Passwords should be changed often to ensure that private and secure files are kept secure.

2. Users who choose to publish home pages on the World Wide Web must identify themselves as the author and provide a means to be contacted. In addition, they must include a disclaimer that the home page content reflects their own views and not necessarily that of the University. Furthermore, any pointers to other web resources must include, within the context of the pointer or its surrounding text, a clear indication as to what a browser will find when arriving at that resource.
3. Users may not change, copy, delete, read or otherwise access files or software without permission of the custodian of the files or the system administrator. Users may not bypass accounting or security mechanisms to circumvent data protection schemes. Users may not attempt to modify software except when intended to be user customized.

4. Users may neither prevent others from accessing the system nor unreasonably slow down the system by deliberately running wasteful jobs, playing games, engaging in non-productive or idle chatting, or sending mass mailings or chain letters.

5. Users shall assume that any software they did not create is copyrighted. They may neither distribute copyrighted proprietary material without the written consent of the copyright holder nor violate copyright or patent laws concerning computer software, documentation or other tangible assets.

6. Users must not use the computer systems to violate any University policies or any local, state or federal laws.

7. A user shall disclose to the appropriate authorities misuses of computing resources or potential loopholes in computer systems security and cooperate with the systems administrator in the investigation of abuses. In connection with inquiries into possible abuses, the University reserves the right to examine files, programs, passwords, accounting information, printouts or other computing material without notice.

4.3 Penalties

4.3.1 Abuse or misuse of computing services may violate this policy or user responsibility, but it may also violate the criminal statutes. Therefore, the University will take appropriate action in response to user abuse or misuse of computing services. Action may include, but not necessarily be limited to:

1. Suspension or revocation of computing privileges. Access to all computing facilities and systems can, may, or will be denied;
2. Reimbursement to the University for resources consumed;
3. Other legal action including action to recover damages;
4. Referral to law enforcement authorities;
5. Computer users (faculty, staff and/or students) will be referred to the appropriate office for disciplinary action.

5 Additional References

6 Authority

The UNC Policy Manual, Chapter 100.1, The Code, Section 502

7 Contact Information

8 Original Effective Date

9 Revision Dates

June 21, 2017