AUP - Individual and University Responsibilities

Acceptable Use Policy – Individual and University Responsibilities

Responsibilities of Users

Account holders are responsible for adhering to this Acceptable Use Policy.

Account holders are responsible for anything done with their accounts. Therefore passwords should never be displayed or shared, should be chosen judiciously, and changed often. If a user suspects account security has been violated, the password should be changed immediately and IT notified immediately.

The user is responsible for correct and sufficient use of the tools available for maintaining the security of information stored on each computer system. The following precautions are strongly recommended:

- Computer accounts, passwords, and other types of authorization that are assigned to individual users should not be shared with others.
- The user should assign an obscure account password and change it frequently.
- The user should understand the level of protection each computer system automatically applies to files and supplement it, if necessary, for sensitive or confidential information.
- The computer user should be aware of computer viruses and other destructive computer programs, and take steps to avoid being a victim or unwitting distributor of these processes.
- Primary responsibility for resolution of problems related to the invasion of the user's privacy or loss of data rests with the user.
- The computer user should consider whether information distributed using University resources should be protected from unauthorized use by the use of copyright notices or by the restriction of distribution of certain materials to the campus.

Responsibilities of the University

The University, through The Office of Information Technology, is responsible for providing central system and network security and for taking reasonable steps to protect central systems and networks and the information stored thereon from excessive or inappropriate use, damage, or destruction. These responsibilities include:

- Instructing, encouraging, and, for critical systems, forcing users to select reasonably secure passwords and to change them periodically;
- Implementing measures to protect systems from hacking, invasion, viruses, trojan horses, and similar threats, and maintaining these measures at a reasonably current level;
- Removing any viruses or other malicious software that may be found on central systems;
- Monitoring use of systems and networks for traffic volume, log activity, or other symptoms of excessive or unauthorized use;
- Promptly taking appropriate measures to halt unauthorized or inappropriate use including, if necessary, imposing appropriate resource allocations or restrictions;
- Performing regular backups of centrally-stored information and maintaining these backups for a reasonable length of time;
- Periodically removing selected backups to a safe off-site location;
- Diligently pursuing and working with other interested offices, departments, agencies, vendors (within the University or outside the University) to resolve violations of the Acceptable Use Policy or other threats to the availability and security of University computing resources;
- Advising owners and custodians of other University computing resources on the manner and means of accomplishing these objectives with respect to the systems they manage.

Version	Date	Comment
Current Version (v. 4)	**Sep 14, 2017 17:48**	**Unknown User (rklein)**
v. 3	Sep 14, 2017 16:50	**Unknown User (rklein)**
v. 2	Sep 14, 2017 16:35	**Unknown User (rklein)**
v. 1	Sep 14, 2017 16:35	**Unknown User (rklein)**