IRA A. FULTON SCHOOLS OF engineering

SSEBE RA / TA – Information & Technology Policies

a condition of employment within the School of Sustainable Engineering and the Built Environment, all student hourly workers are ected to meet with the Information and Technology policies described below.

- Back up important documents to a secure drive, not to the desktop.
- Consult with Alan Short (alan.short@asu.edu) or Jeff Ahlstrom (jeffrey.ahlstrom@asu.edu) concerning software installation c other computer hardware/software/network questions.
- SPP 801: Employee Conduct and Work Rules: Inappropriate behavior as described by the regulations will result in **disciplinar action up to and including termination of employment**. Inappropriate behavior that may result in disciplinary action include direct or indirect use or misuse of university resources, including university computing and communication resources, includi computers, networks, electronic mail services, electronic information sources, voice mail, telephone services, and other communication resources.

Prohibited Uses of ASU Computing and Communications Resources

(as described in ACD 125: Computer, Internet, and Electronic Communications)

1. Unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications, are prohibited.
2. Use of ASU computer resources for private business or commercial activities, or for fund-raising or advertising on behalf of n ASU organizations, is prohibited.
3. The unauthorized reselling of ASU computer resources is prohibited.
4. Unauthorized use of university trademarks or logos and other protected trademarks and logos is prohibited.
5. ASU Web pages may link to commercial Web sites, but any link that generates, or has the potential to generate, revenue to A or to any individual or company, including click trade or banner advertising, must be approved by Purchasing and Business Services.
6. College and department Web sites may include links to commercial Web sites to provide information related to the mission c function of the college or academic or administrative unit. Any link that generates, or has the potential to generate, revenue the college or academic or administrative unit must be approved through Purchasing and Business Services.
7. Any alteration of addresses, uniform resource locator (URL), or other action that masks the asu.edu domain as a host site is prohibited unless authorized by the UTO.
8. Unauthorized anonymous and/or pseudonymous communications are prohibited. All users are required to cooperate with appropriate ASU personnel or other authorized personnel when investigating the source of anonymous messages.
9. Misrepresenting or forging the identity of the sender or the source of an electronic communication is prohibited.
10. Unauthorized attempts to acquire and use passwords of others are prohibited.
11. Unauthorized use and attempts to use the computer accounts of others are prohibited.
12. Altering the content of a message originating from another person or computer with intent to deceive is prohibited.
13. Unauthorized modification or deletion of another person's files, account, or news group postings is prohibited.

Prohibited Uses of ASU Computing and Communications Resources (continued)

(as described in ACD 125: Computer, Internet, and Electronic Communications)

14. Use of ASU computer resources or electronic information without authorization or beyond one's level of authorization is prohibited.
15. Interception or attempted interception of communications by parties not authorized or intended to receive them is prohibit
16. Making ASU computing resources available to individuals not affiliated with ASU without approval of an authorized ASU offic at or above the level of dean or director is prohibited.
17. Intentionally or recklessly compromising the privacy or security of electronic information is prohibited.
18. Infringing upon the copyright, trademark, patent, or other intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction) is prohibited. The unauthorized storing, copying or use of audio files, images, graphics, computer software, data sets, bibliographic records and other protected property is prohibited except as permitted by law.
19. Interference with or disruption of the computer or network accounts, services, or equipment of others is prohibited. The intentional propagation of computer "worms" and "viruses," the sending of electronic chain mail, denial of service attacks, a inappropriate "broadcasting" of messages to large numbers of individuals or hosts are prohibited.
20. Failure to comply with requests from appropriate ASU officials to discontinue activities that threaten the operation or integr of computers, systems or networks, or otherwise violate this policy is prohibited.
21. Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer a network access without authorization is prohibited.
22. Altering or attempting to alter files or systems without authorization is prohibited.
23. Unauthorized scanning of networks for security vulnerabilities is prohibited.
24. Attempting to alter any ASU computing or networking components (including, but not limited to, bridges, routers, and hubs) without approval or beyond one's level of authorization is prohibited.
25. Wiring, including attempts to create network connections, or any extension or retransmission of any computer or network services unless approved by an authorized network administrator is prohibited.
26. Negligent or intentional conduct leading to disruption of electronic networks or information systems is prohibited.
27. Negligent or intentional conduct leading to the damage of ASU electronic information, computing/networking equipment, ar resources is prohibited.

dent Name:_____

_____ acknowledge that I have read, understood, and agree to follow the SSEBE IT Policies.

e: