ECEE IT POLICIES

The following document outlines the policies of the IT department for ASU's School of Electrical, Computer, and Energy Engineering (ECEE). All persons using ECEE owned computer equipment or requesting service from ECEE IT must adhere to these policies.

COMPUTER EQUIPMENT PURCHASES

Per ASU purchasing policy, **all** computers, monitors, and printers purchased **must** meet the EPEAT Gold standard (http://www.asu.edu/aad/manuals/pur/pur210.html [items 1 & 2 under "ENERGY"]). You can see a list of EPEAT compliant computers at http://www.epeat.net/. ASU has made a public statement and commitment that 100% of the computers, monitors, and printers purchased are EPEAT Gold certified. This statement can be found here: https://stars.aashe.org/institutions/arizona-state-university-az/report/2014-02-28/OP/purchasing/OP-12/

All Computer Equipment purchases must come through ECEE IT for approval. This is to ensure compliance with mandates from the Information Security Office, ASU's EPEAT Gold standard policy, and that peripherals are compatible with current system configurations. ECEE IT gives preference to enterprise level hardware, especially those manufactured by Dell and Apple, Dell being our primary and preferred computer provider. After a purchase is made, equipment should be delivered to GWC 208, allowing ECEE IT to install or configure the equipment to comply with ASU's computing and security policy.

It is highly recommended that computer equipment be purchased from a preferred vendor and the portal that those vendors have provided to ASU. If not purchasing from these vendors or their venues, purchases must be made from the department level (using a P-Card), regardless of price. This is to ensure that the University is seen as the owner of the equipment by the vendor/manufacturer.

All desktop computers approved by ECEE IT will include a mouse and keyboard. Equipment that has not been approved prior to purchase by ECEE IT will be given limited support.

For computers leaving the Premises, an off campus loan form must be filled out in advance. These forms can be found at http://www.asu.edu/purchasing/forms/temp_off_campus_loan.pdf and must be submitted every two years, or the equipment should be returned to ECEE IT. This is to ensure both ASU and ECEE IT are aware of the general location of ASU purchased and owned computer equipment. Once this information is filed with ECEE IT you may visit the following site to see the information that has been logged for you and your offsite equipment: https://fulton.sp10.asu.edu/ecee/Off%20Campus%20Loan%20Forms/Forms/AllItems.aspx.

Donations of computer equipment to ASU should be handled according to the policies and procedures described on the following website: http://www.asu.edu/aad/manuals/pcs/pcs405.html

COMPUTER EQUIPMENT SALVAGES

Requests for salvage pickup of computer equipment can be submitted at http://links.asu.edu/ECEEIT-REQ. All computer equipment that is to be salvaged should be kept in the room of original location until ECEE IT can

remove it. This is in accordance with Fire Marshal regulations, keeps the halls free of clutter, and deters theft of equipment. ECEE IT will fill out all required paperwork.

SOFTWARE

NON-STANDARD INSTALLS

ECEE IT will default to the licensed software standards that UTO and ETS has put into place and supports through their infrastructure(s). If a tool is already paid for and provided by the University, ECEE IT will standardize on that tool (such as Outlook for email) and provide limited to no support for alternative software solutions.

PURCHASES AND LICENSING

Software purchase requests should come through ECEE IT. ECEE IT may already have the requested software (or a comparable alternative) freely available to use on an ASU machine, and in some cases a home/personal computer as well.

Regardless of method of purchase, all software installed on ASU computers must be property of ASU (not the user) or ASU must have license to run the software. If the software is purchased, a copy of the receipt of purchase must be on file with a department admin. Specialized software used for research and licensed to an individual faculty will be handled on a case-by-case basis in consultation with ECEE IT. This is to ensure compliance with technology audits put forth by ABOR and to stay in good standing with the agreements that ASU has with various software manufactures. Additionally, ECEE IT will not loan out or allow end users to retain installation media.

RUSH JOBS AND TRAVEL ISSUES

In cases of rush jobs, ECEE IT will do their best to finish a task in the most timely manner. However, ECEE IT cannot guarantee completion of any job faster than 3 business days.

It is the responsibility of traveling Faculty and Staff to plan accordingly for their trips. Computer issues should be resolved at least 2 weeks before traveling to ensure computer equipment will be prepared for travel.

COMPUTER LOGINS

All ASU computers that connect to the network must be on the domain. This ensures a secure login (sans infected computers), network resources are more readily available on demand, and OS updates are managed. These computers are not allowed to have generic or local logins. This means that all students should be logging in through ASUAD and all Faculty and Staff (including student workers) should be logging in through ASURITE.

Computers not connected to the network are not required to be on the domain and may use generic or local computer accounts.

Apple computers are not connected to the domain and are currently exempt from any restrictions that may have been mentioned on the matter.

ADMINISTRATIVE PRIVILEGES

The granting of administrative privileges to a user on a specific computer is delegated to the supervisor (the faculty advisor in the case of graduate students). Administrative privileges are not the standard operating mode but are granted on the supervisor's discretion to enable/facilitate performance of certain ASU-related functions. Both the supervisor and the employee will be held accountable for their actions while these privileges are exercised. Because of this accountability, there are certain situations that will result in a revocation of administrative privileges and the ability to delegate those privileges, as follows:

ACCOUNTABILITY OF EMPLOYEES

Employees, students, postdocs, etc. are accountable for the actions that they take on their computers while having administrative privileges granted. The following will be used to enforce that accountability:

PIRACY

Pirating software is illegal; it can have major legal repercussions on the individual and the University. There are very few cases where pirating is not intentional. Additionally, it is rare when piracy is not accompanied by malware. Therefore, piracy will be dealt with in the following manner:

- 1st offense
    - Verbal and electronic warning to the offender and informing message to the supervisor
    - 24 hours given to backup all important ASU related information
    - Computer will be wiped, offending material removed, and OS re-installed
    - Administrative privileges revoked for 6 month
- 2nd offense
    - Verbal and electronic warning to the offender and informing message to the supervisor
    - 24 hours given to backup all important ASU related information
    - Computer will be wiped, offending material removed, and OS re-installed
    - Administrative privileges revoked permanently
- If it is found that the computer has pirated software on it that is downloaded through malware (i.e. the user is not completely at fault for the pirated software), the procedure for dealing with malware will be followed.

MALWARE

Though malware infections are hazardous to data in a plethora of ways, usually the infection is not a deliberate, intentional infection. Because of this, malware will be dealt with in the following manner:

- 1st offense
    - Warning is issued to employee
    - Supervisor informed of offense
    - Data is backed up and computer is wiped and given a fresh install of the OS and applications
- 2nd offense

    - Supervisor is informed of the second offense
    - Data backed up, computer wiped and given a fresh install of the OS
    - Offender admin privileges revoked for 6 months
- 3rd offense
    - Supervisor is informed of the third offense
    - Data backed up, computer wiped and given a fresh install of the OS
    - Removal of admin privileges will be permanent

Accountability of Supervisors

Because the granting of administrative privileges is delegated to the supervisors/faculty advisors, they will be held accountable for the actions of their employees that are granted administrative privileges. If a supervisor's employee(s) have offenses in this area, the following procedures will be followed:

For every 3 offenses, the supervisor's ability to assign administrative privileges will be revoked for a semester. If the supervisor's privileges are revoked beyond a year, the matter will be taken up with the director of ECEE for further action.

Accountability of Other Parties

Administrative privileges may be granted to those that are not deemed an employee (i.e. visiting researchers, graduate students, etc.). These individuals, though not an employee, will be held accountable as if they were. Faculty advisors for these individuals will be viewed as the supervisor.

Reinstatement of Privileges

Administrative privileges that have been revoked may be reinstated through a petition to the school Director or her/his delegate.