ECE MANAGEMENT PROCEDURES FOR COMPUTING DEVICES USED FOR RESEARCH AND TEACHING

GOAL:

To assist ECE faculty, staff and students comply with University policies governing the use of Information Technology (IT) devices, to document the degree of compliance to those policies within ECE, and to educate members of the ECE community on how to improve the security of their devices and how to protect sensitive information.

PRINCIPLES

1. The ECE community generally operates its IT infrastructure in compliance with University policy. Moreover, when our faculty, staff and students are simply told what needs to be done (and given the tools and assistance necessary to do it), our community has proven both very willing and very capable at adapting their computer use to meet ECE or UT requirements.
2. Given that unsecured computers and unauthorized use is the exception and not the norm, the compliance activities relating to information technology in the department will largely be focused on documenting how current usage satisfies UT and ECE requirements. That effort will no doubt discover systems and uses of those systems that are violating established policies. We should invest our resources to remediate and assist in the management of only those systems which are discovered to be out of compliance.
3. Different types of systems pose different levels of risk. A compromised server is likely to be far more disruptive than a compromised cell phone. The theft or unauthorized release of UT Confidential data is potentially far more impactful than the unintentional release of UT Published data. Our third principle is that IT policy should have a posture consistent with the level of threat. For example, the oversight and compliance activity relating to computer servers will likely appear more intrusive than the oversight and compliance activity relating to tablets or mobile devices.
4. Complying with University policies is not optional, and while the majority of computing usage is consistent with UT and ECE policies, there have been cases within ECE where systems are configured and/or used in a manner that violates University policy and/or potentially undermines the reputation of the ECE department or interferes with ECE activities and operations. ECE must step up and meet its responsibility to better document the degree of compliance to policy and to detect and remediate systems and usage patterns that are failing to comply.

POLICY ELEMENTS

The recommendations and requirements outlined in this document apply to any device (e.g., laptop, desktop, server, tablet, etc.) that is UT-owned, and apply to that device regardless of where that device is located. In addition, the recommendations and requirements also apply to privately-owned devices that are connected to the ECE network either directly or via The University's Virtual Private Network (VPN) service. The only exceptions are those specifically noted below.

PURCHASING AND DEPLOYMENT OF EQUIPMENT

The ECE network is a University resource, and use of the network requires appropriate authorization. Under the policy outlined in this document, ECE faculty are able to authorize their own direct use, and also authorize their students, postdoctoral researchers, research staff and teaching assistants to use the ECE network and/or University-owned computing devices. For example, Graduate Research Assistants are permitted use of ECE computing equipment and can connect their devices to the ECE computing equipment only after receiving authorization to do so from their supervising professors.

Before granting his or her authorization, a faculty member must take reasonable steps to ensure that the device will be properly configured and administered and that all users of the device understand their responsibilities under the rules of The University. These steps include at least two phases of interaction with the ECE IT professional staff as follows:

1. Prior to purchasing any new computing, networking, information storage, or printing equipment with University funds and where that equipment would be connected to the UT network or other public internet access provider, the faculty member must ensure that ECE-IT staff have confirmed that the equipment can be reasonable configured and secured according to UT policy. This pre-purchase approval can be accomplished by selecting equipment from a list of pre-approved standard equipment maintained by the ECE IT staff and/or may be accomplished by providing the ECE IT staff with a standard form that indicates the type of device, its features and capabilities and the measures by which that device can be configured and secured (e.g., the specifics of the operating system and encryption method that will be used).
2. After the equipment is received by UT and prior to putting the equipment into service, the faculty member must ensure that the equipment is properly recorded in the IT and University inventory systems, and ensure that the device has been properly configured consistently with all ECE and UT policies. This pre-deployment configuration and inventory process can be accomplished by delivering the equipment to the ECE IT professional staff where it will be configured and returned to the faculty member in a timely fashion. The pre-deployment configuration may alternatively be accomplished by the faculty member himself or herself, or by a trained member of the faculty member's research group (e.g., a graduate student), provided that trained individual has satisfied ECE and UT's IT training requirements. Regardless of the individual performing the pre-deployment configuration, all new equipment must be fully configured to comply with all ECE and UT policies before being put into operation.

Note that if an existing piece of equipment is being redeployed (e.g., assigned to a new student to use), then the pre-deployment step (step 2 above) must be followed. Similarly, if a new operating system image is to be installed on an existing system, whether or not this installation is part of a hardware upgrade, then the pre-deployment step must be followed. In some cases, computing systems may be constructed from components purchased (or donated to UT) at different times, or components repurposed from other systems. In such cases, the pre-deployment step must be followed when a new operating system image is installed on a computing device (even if a pre-purchase step did not apply).

Should the IT staff determine that a system on the ECE network is not configured consistently with ECE expectations and/or being used in a manner that violates University terms of use, the authorizing faculty member will be the primary point of contact for IT staff when attempting to investigate and correct the issue. Consequently, in the policy elements that follow in this document, the term "responsible faculty member" of a particular computing device refers to the faculty member who has authorized the use of that device. In this context, the term "responsible" indicates that the faculty member has knowledge of how the device was intended to be used, and is able to justify why the intended use of that device on the ECE network is consistent with the mission of the ECE department. In the event that a graduate student or other third party has used a computing device for activities other than its intended use, this policy does not imply any responsibility for such activity beyond what is already required by University rules for the supervision of research students and staff.

EXPECTATIONS

All computers will be operated with full compliance to University Policies, this includes at a minimum

- All devices connected to the ECE network will be cataloged in the ECE IT inventory system, which will include information about the device (device type, network address(es), operating system type and version, etc.) and will identify the faculty member who authorizes use of this device on the ECE network (the "responsible faculty member").
- Each account on each computer will be secured with a strong password.
- The disk drive of any University owned computer system will be encrypted using an approved whole-disk encryption method. Privately-owned laptops are required to be encrypted when it is possible that the device will be used to access UT Confidential data (e.g., to review or submit grade information).
- The document storage on any tablet or mobile device will enable data security features (e.g., encryption) available on that device and will have the remote wipe capability enabled. For example, Apple (IOS) tablets should be secured following the checklist at https://wikis.utexas.edu/display/ISO/Apple+iOS+Hardening+Checklist
- An active anti-virus system will be operated on all desktop and laptop computer systems (mobile devices such as tablets and phones are currently exempted).
- A fully supported operating system will be used, and security updates will be installed in a timely fashion.
- All software applications and utilities will have current licenses and will be used in accordance with the End-User Licensing Agreement (EULA) and/or Terms of Use for the software.
- Laptops and mobile devices will be configured to require a password when resuming from suspend or when exiting the screen saver.
- All documents produced as part of University activities, including but not limited to research results, publications, teaching materials, exams, grades, administrative records,

budgets, proposals, and the like will be backed up using a backup method appropriate for the type of information being saved. For faculty data, UT Backup (i.e., Crashplan Pro) is recommended for this purpose. It is strongly recommended that any security keys (i.e., encryption passwords) that apply to the backup will be appropriately escrowed to ensure that critical data can be recovered.[1]
- All systems and components of systems that have reached their end-of-life or for any reason are being discontinued from use will have their storage systems wiped and will be disposed of using appropriate procedures. ECE IT staff can assist with the decommissioning and/or disposal of computing devices.

Where such practices do not interfere with achieving the mission goals of the department, the following additional expectations apply to computing devices and networks operated within ECE

- Computer systems (desktops and laptops) will be configured to require a password when resuming from suspend or when disabling the screen saver. Note that this configuration is mandatory for all computers located in public areas, shared offices, or open workspaces (i.e., cubicles).
- Laptop and desktop computer systems will be configured to not provide administrator rights to the primary account for a user. Users may have administrator rights on a secondary account that can be used to install software and run some programs requiring administrator rights. Email and web applications will not generally be used from within accounts that have administrator rights.
- In publicly accessible open areas (e.g., cubicles), desktop computers and University-owned laptops left in fixed locations will be physically secured with a security cable or similar locking device to discourage theft.
- Servers that provide commodity services will be housed in the University Data Center (UDC).

It is strongly recommended that that privately owned devices, when these devices are used for University purposes, be configured and used as required of University-owned computers. Note that configuration and use consistent with these expectations is mandatory for any privately-owned devices that are directly connected to the ECE network and/or connected to The University VPN service. Failure to meet minimum security standards and/or security breaches for any reason can lead to quarantine from ECE networks as described below.

COMPLIANCE

ECE IT staff will assist ECE faculty and their designees (e.g., admin staff, research staff, postdocs, graduate and undergraduate research assistants) to comply with University and department guidelines for computer use by:

- Prepare and conduct IT-training sessions for ECE graduate students who may have computer administration responsibilities assigned to them by their supervising professor.

[1] The method of escrow must meet University security guidelines. In particular, the keys used to protect Category 1 data are considered to be Category 1 data. Hence, the escrowed keys for Category 1 data must themselves be encrypted and/or stored in an appropriately secured location. The UT stache service is an example of an acceptable escrow mechanism.

These training sessions will be offered every semester and will describe UT and ECE requirements as well as industry best practices for administration of computing devices. IT staff will also identify and provide recommendations for external training materials for the benefit of graduate students and faculty members administering UT computing equipment. These external training resources may include online courses, UT-administered compliance training modules, and/or canvas-hosted interactive "courses".

- Implementing the pre-purchase and pre-deployment checks that ensure UT-owned equipment is appropriate for its intended use, can be adequately secured in accordance with UT policies, and is correctly configured before being placed into service.
- Assisting in configuring and maintaining University-owned systems as needed.
- Monitoring the department network to ensure that systems are complying with minimal security guidelines.
- Conducting surveys and periodically meeting with faculty and faculty-designated students to discuss usage patterns and procedures.

GRADUATE STUDENT PRIMARY ADMINISTRATORS

ECE will leverage graduate students as part of its IT oversight. ECE faculty may identify one or more graduate students as "primary student administrators" for the faculty members' research group. All primary student administrators must receive regular IT training (see below), and will be expected to act as the IT-staff's primary contact point for pre-deployment checks, security audits and compliance activities within that research group. If a faculty member declines to designate as primary student administrator, then the faculty member himself/herself must either fully administer (be the sole person with administrator privileges) for all computing equipment used by the research group, or must authorize ECE-IT to administer that computing equipment.

In cases where a primary student administrator is designated by a faculty member, that individual's authority to administer ECE systems is constrained as defined below and will only apply to computing devices which are under the responsibility the supervising faculty member. In no cases will a graduate student be given administrator privileges on any ECE teaching laboratory or ECE core IT infrastructure (e.g., web server, file hosting services, ECE network administration, etc).

USE OF ADMINISTRATOR ACCOUNTS

ECE subdivides computing equipment into two categories; single-user devices and multi-user devices. A multi-user computing device is any computer running a multi-user operating system where two or more individuals routinely log into the device and/or a device where University data produced by two or more individuals is stored on the device. Any device that is not a multi-user computing device is deemed to be a single-user device. The following examples help illustrate this distinction

- A computer server providing specialized applications (e.g., Computer Aided Design software) for the benefit of multiple students and/or faculty is a multi-user computing device.
- A file server which collects data for a research group, including the data from multiple students is a multi-user computing device.

- A desktop computer running Linux (a multi-user operating system), where only a single person uses the device on a day-to-day basis, and where no internet services (e.g., mail, web, database, file storage) are hosted on the computer is a single-user computing device.
- All phones and tablets are single-user devices.
- Most laptop computer are single-user devices, regardless of operating system

Single-user devices and multi-user devices are subject to different policies with regard to administrator privileges. This distinction is in accordance with the principles of this policy where greater protection and oversight is appropriate when greater risk exists. Regardless of whether a system is a single-user device or a multi-user device, ECE-IT will record in its IT-inventory all administrator accounts on the device including the name, login name and UTEID of the administrator. This information is collected as part of the pre-deployment check of computing devices in ECE.

ADMNISTRATION OF SINGLE-USER DEVICES

Faculty will retain administrator rights on any single-user device that they operate, provided the faculty member agrees to abide by all ECE policies for configuring the machine, agrees to subject the machine to periodic audits by ECE IT Staff for compliance, and provided the faculty member signs (annually) the UT acceptable use policy for IT equipment.

Graduate students will be permitted to retain administrator rights for single-user, university-owned devices provided the device is known in advance to have been correctly configured to comply with UT and ECE policies, and provided an IT-trained representative also retains administrator rights to the computer for the purposes of conducting compliance checking. The IT-trained representative may be member of the IT staff or may be a graduate student that has participated in the ECE IT training seminar for graduate students.

Staff members will generally not be provided with administrator access to computers. Exceptions will be reviewed by the ECE-IT committee and may be granted on a case-by-case basis. If a staff member is provided with administrator access IT-trained representative will also retain administrator rights to the same device for the purpose of conducting compliance checking.

ADMINISTRATION OF MULTI-USER DEVICES

All multi-user devices must be assigned a primary administrator. This primary administrator may be a faculty member, a member of the ECE-IT staff or may be a graduate student. If a primary administrator is a graduate student, then that student must have participated in the ECE training seminar for graduate students. The primary administrator of the device must regularly monitor the device to ensure data stored on the device is secure and that the device is properly configured. ECE-IT may mandate periodic reports be provided by the primary administrator to ensure the device is being properly maintained. These reports may include the following information

- A log of all privileged accesses (e.g., sudo privilege elevations) performed on the device
- An update history documenting when the last operating system updates/patches were applied
- A configuration status for all services (if any) provided by the machine including login (e.g., SSH), mail (e.g., sendmail), web or database (e.g., Apache). Changes to configuration of services should be made only in consultation with the ECE IT staff.

In addition to the primary administrator, other individuals (ECE faculty, IT staff or graduate students) may be provided with administrator access on multi user machines. In the case of a graduate student with administrator privileges on a multi-user device, then that student must have participated in the ECE training seminar for graduate students.

GRADUATE STUDENT IT TRAINING

ECE will leverage its limited IT resources by delegating certain tasks to graduate students. The use of graduate students in IT operations is limited to computing resources within the graduate students' own research group (i.e., devices and equipment overseen by the students' supervising professor) and is subject to the limitations described elsewhere in this document. In addition, graduate students who either (a) have administrator access to a multi-user computing device, or (b) are given responsibility as a primary student administrator for a research group, must have received special training from ECE IT staff and must periodically refresh their training to ensure these students are qualified to act as an IT representative. This training will include a review of ECE and UT policies for configuration and administration of single-user and multi-user computers, and recommended best practices for administration of devices.

Each long semester, ECE IT will conduct at least two training seminars. Graduate students are expected to participate in at least one of these semesters every calendar year. Only students that have participated in a training seminar will be permitted to retain administrator access to any multi-user computing device within ECE or to act as the primary student administrator for a research group. If a graduate student has taken the training seminar in the past, but has not taken a seminar within the last three long semesters, or has not taken at least two training seminars in the last four long semesters, then that student's training will be deemed to have lapsed, and the student will be denied administrator privileges and may not be assigned IT responsibilities until the training has been retaken.

FACULTY IT COMMITTEE

To support the implementation of this policy and to assist the IT staff in their mission to improve IT use in ECE, the department has created a standing committee of faculty called the ECE Faculty IT Committee. This committee will include broad representation from across the ECE technical areas. Each technical area is invited to nominate a representative to serve on the committee to the ECE department chair. Subject to approval by the ECE department chair, these nominated individuals will serve on the Faculty IT Committee for a period of at least one year, and may be re-nominated and reappointed at the conclusion of that term. The responsibilities of the committee include:

1. Periodically reviewing and updating the ECE guidelines for securing computing devices and ensuring that the corresponding checklists are correct and easy to follow. These guidelines are intended to ensure compliance with all University requirements and any additional ECE expectations for use of computing devices. Over time those requirements will change and new technology will be developed which will necessitate revisions to the ECE guidelines. The Faculty IT Committee will approve any revisions.
2. Grant exceptions to the ECE guidelines and to this policy when (1) such exceptions do not violate University policy, and (2) the exception is in the best interest of accomplishing the research or teaching goals of the faculty and department.

Decisions within the Faculty IT Committee will be made by simple majority vote. The chairman of the committee will not vote. In the case of an impasse, the committee chairman will cast a vote to resolve the impasse. Decisions of the Faculty IT Committee regarding which systems are authorized to be used on the ECE network and the circumstances by which those devices shall be used are binding. Faculty members who do not agree with a decision by the Faculty IT Committee can seek redress from the ECE Chairman's office.

EXCEPTIONS

The policies in this document apply to all University-owned equipment purchased by and/or operated by students, staff and faculty in ECE. Exceptions to these policies are necessary in some specific cases due to the nature of the research and education performed within ECE. Some ECE curriculum involves the design and construction of small embedded computer systems (e.g., deployed within a robot) in which the computer system has WiFi network connectivity to the internet. Such connectivity is necessary for the installation of device drivers and may also be necessary for the operation of the device. Research within ECE often involves computer network analysis and experimentation, the design, study and experimentation of distributed computing systems, high-performance parallel computer systems, and may other forms of computing and networking.

In cases where the use of a device or devices in ECE education or research cannot be reconciled with the policies in this document, then the ECE Faculty IT committee can grant exceptions to those devices. The following guidelines are provided to the committee regarding the sorts of exceptions that are reasonable and appropriate. Note that any exceptions must be documented and referred to the UT ISO.

- Use of Firewalls – in most cases, when an exception is requested, the use of the device or devices should be conducted in a manner where the devices are shielded from the network behind a firewall. In cases where internet access is required only temporarily, the device or devices should be disconnected from the internet when possible.
- Proper sequestration of data – Devices for which exceptions are being requested should be special-purpose devices. General purpose computing, including such tasks as reading email, conducing literature surveys or internet searches, etc. should be conducted on standard devices. In particular, devices should collect and store only the data necessary for the devices to be used for their intended purposes.
- Shared accounts – UT policy provides that each account/login used to access a computing device should be associated with a single individual. Exceptions to this policy are sometimes necessary, but should be granted only when strong protections are otherwise in place for the device. These protections should include such elements as physical security to the device, very limited data storage on the device (ideally no data should be stored on a device with shared accounts, and any such data that is collected by the device should be only stored temporarily on the device before being transferred to another more appropriate device or media), limited access to the internet (especially limited incoming access to the device from the internet – e.g., no remote login)