6-12-2023

2023 June 12 -- University Council Agenda and Minutes

East Tennessee State University

AGENDA
University Council

Monday, June 12, 2023
East Tennessee Room
8:30 a.m. – 11:00 a.m.

1. Call to Order
2. Roll Call
3. Standing Items
   - 3.1. Approve minutes of the April 10, 2023 meeting *(*attachment*)*
   - 3.2. Review agenda
   - 3.3. Consent agenda items:
     - 3.3.1. General Purchasing Policy (attachment)
     - 3.3.2. Hazardous Energy Control (Lockout/Tagout) (attachment)
     - 3.3.3. Acceptable Use of Information Technology Resources (attachment)
     - 3.3.4. Building Access Control Policy (attachment)
     - 3.3.5. Fire Protection and Life Safety Policy (attachment)
   - 3.4. Call for Voluntary Reports of UC-Essential Action Items from Governance Organizations
   - 3.5. Sub-Council Reports – Budget and Strategic Planning Committee – Christy Graham
4. Action Items
   - 4.1. Old Business
   - 4.2. New Business
5. Information Items/Presentations
6. President's Report
7. Announcements
8. Adjournment

The next meeting is scheduled for July 10, 2023 at 8:30 a.m.

University Council
Monday, June 12, 2023
East Tennessee Room

1. Call to Order

Provost Kimberly McCorkle called the meeting to order at 8:31 a.m.

2. Roll Call

Fred Sauceman led the roll call. Members present were: Dr. Ginni Blackhart, Dr. Joe Bidwell, Dr. Cheri Clavier, Dr. Joel Faidley, Ms. Joy Fulkerson, Ms. Christy Graham, Dr. Adam Green, Dr. Lisa Haddad, Dr. Nick Hagemeier, Mr. Steven Hendrix, Dr. Mike Hoff, Dr. Karen King, Ms. Candy Massey, Dr. Sam Mayhew, Dr. Kimberly McCorkle, Dr. Rob Pack, Ms. Pam Ritter, Dr. Janna Scarborough (via Zoom), and Dr. Joe Sherlin.

3. Standing Items

3.1 Approve minutes of the April 10, 2023, meeting

A motion was made to approve the minutes from the April 10, 2023, meeting. The motion was seconded; the minutes were approved.

3.2 Review agenda

There were no changes to the agenda other than the elimination of the President's Report, since President Noland is traveling abroad with a group of students.

3.3 Consent agenda items

A motion was made to approve updates to the five policy items listed below as presented. The motion was seconded and approved.

- 3.3.1. General Purchasing Policy
- 3.3.2. Hazardous Energy Control (Lockout/Tagout)
- 3.3.3. Acceptable Use of Information Technology Resources
- 3.3.4. Building Access Control Policy
- 3.3.5. Fire Protection and Life Safety Policy

3.4 Call for Voluntary Reports of UC-Essential Action Items from Governance Organizations

Faculty Senate: Dr. Ginni Blackhart reported that the Faculty Senate is continuing to work on revisions to the Faculty Handbook and that planning is continuing for the senate's August 22 retreat.

Council of Chairs: Dr. Lisa Haddad reported that the Council of Chairs has not met since the last University Council meeting. She also indicated that the Council of Chairs will be undergoing some membership changes.

Staff Senate: Ms. Joy Fulkerson reported that the Staff Senate hosted a successful social and end-of-year celebration. She added that plans are underway for next year's event. A call for nominations for Staff Senate seats will be sent out soon, in preparation for the next election cycle. Officers will be elected in August. Ms. Fulkerson told the council that some senators had expressed concerns about the impact of the change in the payroll system and that the issue will be explored during the next meeting of the Staff Senate, in consultation with Human Resources.

Student Government Association: Dr. Joe Sherlin reminded the council that SGA is in the midst of a leadership transition, after Mason Mosier's two-year term as President. Dr. Sherlin indicated that the new officers are Trent White, President; Brooke Patterson, Executive Vice President; and Skylar Brackett, Vice President for Finance and Administration.

Information Technology Council: Dr. Karen King reported that the Information Technology Council did not meet in June but is scheduled to meet in July. She said that the conversion to Oracle is progressing well and that the last testing cycle is about to begin. Training will start in August.

3.5 Sub-Council Reports

Budget and Strategic Planning Committee: Ms. Christy Graham, Chief Financial Officer, reported that the Budget and Strategic Planning Committee joined President Noland and the ETSU leadership team to take part in the recent central administration budget hearings, with participation from all units across the campus. She emphasized, as was pointed out during the budget hearings, that since the amount of new money the university will receive for the upcoming fiscal year will be very limited, any new initiatives recommended to the president would require funding through reallocations or through new revenue sources.

4. Action Items

4.1 Old Business

There was no old business to come before the council.

4.2 New Business

There was no new business to come before the council.

5. Information Items/Presentations

There were no information items or presentations.

6. President's Report

Because President Noland was traveling internationally with a group of ETSU students, there was no President's Report.

7. Announcements

Dr. Adam Green reported that the Office of University Marketing and Communications won several awards this spring through the annual competition held by the Tennessee College Public Relations Association.

Dr. Nick Hagemeier reported that the Academic Structure Task Force is continuing its work and that the group anticipates a busy fall semester. He added that the university's research mentorship program will be announced in a few days.

Dr. Sam Mayhew reported on a very successful orientation program that was held last week for new students, with over 500 attending, and he announced that a freshman orientation session is scheduled for June 15.

8. Adjournment

Provost McCorkle adjourned the meeting at 8:44 a.m.

EAST TENNESSEE STATE UNIVERSITY

ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES	
Responsible Official: **CHIEF INFORMATION OFFICER**	Responsible Office: **INFORMATION TECHNOLOGY SERVICES**

Policy Purpose

This policy describes the acceptable use of information technology resources and facilities at East Tennessee State University (ETSU or University).

Policy Statement

This policy provides a framework for the appropriate and respectful use of information technology resources. Failure to act responsibly can adversely impact the University. The policy is intended to prevent abuse of resources and to ensure that usage honors the public trust and supports the University's mission.

This policy applies to employees, students, guests, and third parties using, accessing, or integrating with ETSU technological resources, i.e., computing, accounts, and network systems. For example, this policy applies to individuals using ETSU computing devices, or individuals using personal devices connected to the ETSU network or other ETSU resources.

I. SYSTEM SPONSORS AND OPERATIONAL POLICIES.

A. The information technology resources at ETSU serve a diverse population. System sponsors are given discretion to establish reasonable and appropriate requirements applicable to the systems they oversee. For example, on some campus systems, playing of computer games or use of chat programs may be permitted or even encouraged. On other systems, game-playing and chatting may be discouraged or even prohibited.

B. System sponsors, and by the delegation, system managers and information technology facility staff, have discretion to set and revise reasonable usage priorities and operational policies (such as hours of operation, usage time limits, populations to be served, etc.). They may also take such routine steps (i.e., troubleshooting, updating systems, backing up systems, etc.) as may be reasonably necessary for the operation of their systems or facilities.

II. CYBER-CITIZENSHIP

A. Responsibility

1. Use of ETSU information technology resources must comply with ETSU policies, procedures, standards, and all applicable laws and not be used for any personal, for-profit, or unauthorized not-for-profit, purpose.
2. Users must expect variation in what constitutes acceptable use from system to system on campus and must make reasonable efforts to inform themselves about the particular requirements applicable to each system they use. In cases of doubt, it is the responsibility of the user to inquire concerning the permissibility of an action or use, prior to execution.
3. Users should protect systems from misuse and attack by being up to date on security patch installations and maintain the latest version of ITS approved antivirus patterns and definitions.

B. Resource Management

1. To effectively manage information technology resources, priority is given to applications that support the University mission. The system sponsor has the responsibility to manage resources so as to make them available for mission-related applications.
2. Users are expected to comply fully with the instructions of ITS staff, system managers, system sponsors, and the infrastructure sponsor. In particular, users will vacate facility workstations and will surrender other resources promptly when asked to do so.

III. UNIVERSITY RIGHTS

ETSU reserves the right to access, monitor, review, and release the contents and activity of an individual User's account(s) as well as that of personal Internet account(s) used for University business. The University reserves the right to access any University owned resources and any non-University owned resources on University property, connected to University networks and systems, or containing University data. This action may be taken to maintain the network's integrity and the rights of other authorized Users and to protect the infrastructure from spam, viruses, intrusions, malware, and other malicious content. Additionally, this action may be taken if the security of a computer or network system is threatened, misuse of University resources is suspected, or the University has a legitimate business need to review activity or data.

IV. PRIVACY

A. ETSU Privacy Notification

1. ETSU hereby notifies users that email communication and documents stored or transmitted using ETSU resources may be a public record and open to public inspection under the Tennessee Open Records Act. Therefore, pursuant to the Tennessee Public Records Act (T.C.A. § 10-7-501 et seq.), and subject to exemptions contained therein, all records generated or received by ETSU employees, all records owned or controlled by the State, or all records maintained using ETSU resources may be subject to public inspection upon request by a citizen of the State of Tennessee.
2. Users should have no expectation of privacy when using ETSU computing resources, computer accounts, and network resources.
3. The university does not routinely or without cause monitor individual use of these resources; however, the normal operation and maintenance of these resources require the backup and caching of data and communications, logging of activity, monitoring of general usage patterns, and other such activities.
4. Users should be aware that any activity on systems and networks, including documents created, stored, transmitted, or received on university computers and networks may be monitored, logged, and reviewed by university approved personnel or may be discovered in legal proceedings.
5. Users must respect the privacy and usage privileges of others, both on the ETSU campus and at all sites reachable via ETSU's external network connections.
6. Users will not intentionally seek information on passwords. Unauthorized users will not modify files, data, or passwords belonging to other users. Users will not develop or retain programs for these purposes.
7. Users will preserve and protect the privacy, dignity, well-being, and informed consent of all users of information technology systems.

V. SYSTEM SECURITY

A. Users must respect the integrity of computing systems and networks, both on the ETSU campus and at all sites reachable via ETSU's external network connections.
B. Users will not by any means attempt to gain access to a computing system or network without proper authorization, either on the ETSU campus or elsewhere.
C. Users will not attempt to damage or alter hardware or software components of a computing system or network, either on the ETSU campus or elsewhere.
D. Users will not attempt to disable any hardware or software components of a computing system or network via network attacks and/or scans, either on the ETSU campus or elsewhere.
E. Users will use only supported and patched applications and operating systems on University-owned devices. Exceptions must be documented and approved by the Chief Information Officer or designee.

VI. ACCOUNT SECURITY

A. Users must protect the confidentiality of their assigned account credentials by not sharing passwords, PINs, tokens, or other authentication information with anyone, including friends, supervisors, ITS employees, or other employees.
B. Users must use only the accounts, passwords, and privileges associated with their computer account(s) and use those account(s) only for their authorized purpose.
C. Users must report unauthorized account activity or suspected account compromises to the ITS Help Desk and change passwords immediately.
D. Users shall log out from computers, web pages, and other systems when they are not being actively used and not leave active sessions unattended.

VII. COPYRIGHTS AND LICENSES

A. Violation of copyright law or infringement is prohibited by University policy and state and federal law.
B. Software may not be copied, installed, or used on University resources except as permitted by the owner of the software and by law.
C. Users will properly license software and strictly adhere to all licensing provisions, including installation, use, copying, number of simultaneous users, and terms of the license.
D. All copyrighted information, such as text and images, retrieved from University resources or stored, transmitted, accessed, or maintained with University resources must be used in compliance with applicable University branding, copyright, and other laws.

VIII. USER RESPONSIBILITIES.

Access and use of ETSU IT resources are limited to purposes that are consistent with the instructional, research, and administrative goals and mission of the University. Users SHALL:

A. Respect and honor the rights of other individuals with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright, and use of University resources;
B. Use University provided software in a manner that strictly adheres to all licensing provisions, including installation, use, copying, number of simultaneous users, and other terms of the license;
C. Only use University resources for which they have authorization;
D. Control and secure physical and network access to University resources; and
E. Comply with state and federal regulations concerning obscenity and child pornography, state prohibitions on gambling, and restrictions on gaming.

Users shall NOT:

A. Use information technology resources in a manner that violates ETSU policy and/or other applicable policy and laws;
B. Use accounts, access codes, privileges or ITS resources for which they are not authorized or obtain extra University resources or gain access to accounts for which they are not authorized;
C. Use information technology resources in support of agencies or groups outside the University when such use is not in compliance with the mission of the University;
D. Use information technology resources for activities unrelated to the mission of the University when such use prevents or seriously restricts resource usage by persons fulfilling the mission;
E. Use information technology resources to give access to persons who have not and/or could not obtain access to University resources through official ETSU channels;
F. Use any access not specifically assigned to the user;
G. Tamper, modify, or alter any restrictions or protections placed on their accounts, the University's system, or network facilities;
H. Physically damage or vandalize University resources;
I. Deliberately alter the account structure assigned to the user so as to increase system permissions without ITS authorization;
J. Attempt to render the system or equipment inoperative;
K. Attempt to degrade the performance or availability of any system or to deprive authorized Users access to any University resources;
L. Participate in activities that have the intent of monopolizing information technology resources;
M. Connect network devices such as switches, routers, hubs, and wireless access points to the network without prior approval from ITS;
N. Use University resources to introduce, create, or propagate SPAM, PHISHING email, computer viruses, worms, Trojan horses, or other malicious content;
O. Intercept other Users' transmissions;
P. Misrepresent their identity with actions such as IP address "spoofing," email address falsification, or social engineering;
Q. Send email chain letters or mass mailings for purposes other than official University business;
R. Use University resources as an email relay between non-university email systems (routing email through university email systems between two non-university systems);
S. Use without authorization any device or application that consumes a disproportionate amount of network bandwidth;
T. Include or request Sensitive Information be included in unprotected electronic communication (email, instant message, text message, etc.);
U. Transfer or use copyrighted materials without the explicit consent of the owner. The unauthorized downloading, copying, or distribution of materials (i.e., proprietary music, video, software, or database information) via information technology resources is

prohibited;

V. Commit offenses against others including but not limited to:

    1. Harass another using information technology resources.
    2. Impersonate another.
    3. Take or alter another's work without permission.
    4. Assume credit for the work of another.
    5. Interfere in another's legitimate use of information technology resources.
    6. Display obscene material in a public area. Note: Any direct attachment, linkage, or anchoring of such materials to documents viewable by the public is prohibited; or

W. Abuse information technology resources including but not limited to:

    1. Attempt to gain another user's password or to log on as another user.
    2. Permit unsupervised use of an assigned account by any other person.
    3. Use information technology resources for commercial activities except as authorized by the appropriate University administrative official or unauthorized not-for-profit business activities.
    4. Use ETSU web pages for commercial, private, or personal for-profit activities. Examples include the use of web pages advertising services for personal marketing or business transactions, private advertising of products or services, and any activity meant to foster personal gain.
    5. Use commercial logos/icons unless that owner provides a University service, such as dining services. Those pages must contain a notice that the owner provides the service under contract to the University.
    6. Use ETSU web pages for unauthorized not-for-profit business activities. This includes the conducting of any non-University related fundraising or public relations activities, such as solicitation for religious or political causes.

University employees, contractors, temporary employees, student workers, external parties, and others accessing sensitive systems and data shall NOT:

A. Access websites which are not directly related to the conduct of University business while accessing any University system containing sensitive/protected data.
B. Install or use online chat applications, computer games, peer-to-peer file sharing software or other software which is not directly related to the conduct of University business.
C. Transmit, upload, download, or email, sensitive University data to non-University or unapproved systems.

IX. DIGITAL CONTENT PROVISIONS

A. Default Access – The default access to information technology resources (such as files) is to be set to allow the owner read, write, delete, and execute access and to give access to no other person. If the owner of such resources modifies this access to grant others access, such access by another, in itself, is not considered an ethical infraction. However, it is prohibited to use such access to copy another's work and assume credit for it, modify the file of another without explicit verbal or written permission to do so, and/or publicizing its contents without authorization or by modifying the file's contents in a manner unauthorized by the file's owner.

B. Software – ETSU utilizes a wide variety of software, with an equally wide range of license and copyright provisions. Users are responsible for informing themselves of, and complying with, the license and copyright provisions of the software that they use. No software copy is to be made by any user without a prior, good faith determination that such copying is in fact permissible. All users must respect the legal protection provided by copyright and license to programs and data.

C. Content – Regarding intellectual property, ETSU reserves the right to protect copyrights, patents, trademarks, trade secrets, and other legally obtained rights that prohibit copying, trading, displaying, or using without permission. Many of these items may be found by searching networks including the internet, but their presence on these networks does not imply that they are free to use without permission. All content must comply with copyright laws, policies, and regulations detailed in the Federal Copyright Law (Title 17 of the United States Code), and Digital Millennium Copyright Act (DMCA), the Technology, and the Education and Copyright Harmonization (TEACH) Act.

D. Logos – The use of the ETSU logo is acceptable on University hosted web pages.

X. PRIVILEGE

Access to ETSU information technology resources is granted contingent on that access not being misused. If that access is misused, it can be withdrawn at any time. Further disciplinary action may be taken as a result of serious offenses.

XI. RIGHTS TO PRIVACY

A. While ETSU recognizes the role of privacy in an institution of higher learning and every attempt will be made to honor that principle, there should be no expectation of privacy in any message, file, image, or data created, stored, sent, retrieved, or received by use of ETSU information technology resources. ETSU expects all users to obey all applicable policies and laws in the use of information technology resources.

B. Pursuant to state public records law, T.C.A. § 10-7-503 and subject to the exemptions contained therein, electronic files (including email correspondence) which are maintained using ETSU resources may be subject to public inspection upon request by a citizen of the State of Tennessee.

C. The University abides by the Family Educational Rights and Privacy Act (FERPA), which requires

the University to protect the confidentiality of student education records.

D. When sources outside the University request an inspection and/or examination of any University owned or operated information technology resource, and/or files or information contained therein, the University will review the request pursuant to state law and institutional policy, and will release the information when any one or more of the following conditions exist:

    1. When approved by the appropriate University official(s) or the head of the department to which the request is directed;
    2. When authorized by the owner(s) of the information;
    3. When required by federal, state, or local law; or,
    4. When required by a valid subpoena or court order.

NOTE: When notice is required by law, court order, or subpoena, computer users will receive notice of such disclosures (viewing information in the course of normal system maintenance does not constitute disclosure). In all cases, a request for access to any University Information resource by non-ETSU entities will be reviewed by the Office of University Counsel prior to release.

E. Data on University computing systems may be copied to backup media periodically. The University makes reasonable efforts to maintain the confidentiality of the data contained in the backup.

F. The contents of a user's files will typically not be accessed or disclosed except when (1) the owner has set the file permissions to grant others access in accordance with the restrictions noted in this policy, or (2) in the event of any situation listed below.

    1. The system sponsor in charge of a system may require personnel to investigate the system suspected of being used by someone other than its rightful owner.
    2. The system sponsor in charge of a system may require personnel to investigate the system suspected of being used in a manner that violates University policy or federal, state, or local law.
    3. Information traversing the data networks may be intercepted and/or analyzed in conjunction with investigations.

XII. VIOLATION OF THIS POLICY

Violations of this policy may result in one or more of the following.

A. Immediate suspension of any or all of the following: the user's account, network access, and internet access followed by timely review of the charges by the appropriate person or persons.

B. Revocation of the user's computing privileges at ETSU. There will be no refund of any technology access fees.

C. Recommendation users go through the regular disciplinary processes and procedures of the University for the appropriate student, staff, administrator, and faculty category.

D. Recommendation of termination of employment from ETSU for faculty, staff, and

students.

E. Recommendation the violation be turned over to appropriate law enforcement agencies in the case of suspected law violations for criminal and/or civil action.

Authority: The Focus Act § 49-8-203 et. seq; Federal Copyright Law, Title 17 of the U.S. Code; Digital Millennium Copyright Act; Technology, Education and Copyright Harmonization Act; T.C.A. § 10-7-501 et seq; Family Educational Rights and Privacy Act

Previous Policy:

Defined Terms

A defined term has a special meaning within the context of this policy.

ACCOUNT	A combination of username and password that provides an individual with access to an information technology resource.
CONTENT	Any and all text, images, multimedia elements, coding, and other such items posted, transmitted, and/or used by information technology resources.
FACILITY STAFF	Individuals who are authorized to monitor, manage, or otherwise grant temporary access to computing facilities (such as microcomputer laboratories) in which one (1) or more systems are used by either specific populations of faculty, staff, and students, or the entire campus community.
INFRASTRUCTURE SPONSOR	Person responsible for the ETSU information technology resources infrastructure and who is authorized to determine which information technology resources will be acquired and utilized by the University. (Chief Information Officer (CIO)
INFORMATION TECHNOLOGY RESOURCES	Computing systems, networks, electronic storage, communication, and presentation resources provided by ETSU

SENSITIVE UNIVERSITY DATA	Any information that is protected against disclosure, including all data that may contain personal information, protected health information, student education records, customer record information, card holder data, or other confidential information.
SENSITIVE UNIVERSITY SYSTEMS	Any University owned electronic systems that contain Sensitive University Data.
SYSTEM MANAGER	The person(s) authorized by a system sponsor to grant, restrict, or deny user privileges, maintain the system files, inform users of all applicable policies, and generally ensure the effective operation of a system. In some cases, the system manager and the system sponsor may be the same individual(s).
SYSTEM SPONSOR	The individual(s) under whose authority a computing system, local network, or external network connection is funded. Individual computer systems and local networks may be sponsored by faculty members (i.e., using research grant funds), departments, colleges, or other units. In the latter case, the unit administrator is the system sponsor.

Policy History

Effective Date:

Revision Date:

Procedure

Procedure History

Effective Date:

Revision Date:

Related Form(s)

Scope and Applicability

Primary:

Secondary:

Building Access Control Policy	
Responsible Official: **Chief Operating Officer**	Responsible Office: **Office of Administration**

Policy Purpose

This policy specifies when and how Access Control Devices, electronic and/or key access is granted to ETSU facilities.

Policy Statement

ETSU will control access to facilities based on need, required job responsibilities, individual accountability, and Least Privilege. This policy applies to all ETSU facilities users including, but not limited to students, faculty, staff, temporary employees, contractors, vendors, and any other authorized users who access ETSU facilities and properties. Authorized users accessing ETSU properties are responsible for following all university polices, state, and federal laws.

I. Office Responsibilities.

The Office of Administration is responsible for developing, disseminating, and reviewing and/or updating formal, documented ETSU policies for physical access control, and procedures to facilitate the implementation of Access Control best practices.

The Director of ID Services is responsible for administering the Identification Card/Card Reader System, and the Director of Facilities Operations will have the principal responsibility for administering key control for ETSU properties.

The Chief Operating Officer (COO) or designee is the final authority in disputed matters of Identification Cards/Card Reader System and Key Control.

II. Identification Cards.

All faculty, staff, and students will be issued an identification card by ID Services. Security of University Identification Cards and keys are the responsibility of the person to whom the devices are issued. Lost ID's will be replaced at a cost determined by the current ID Services replacement rate. When an

employee begins leave for any disciplinary actions, ID Cards will be deactivated at the onset of the leave and reactivated upon the employee's return to active status. Upon withdrawal from the university, Student ID Cards will be deactivated and reactivated if the student reenrolls. Student ID Cards will be valid for five years from the issue date or graduation, whichever occurs first. Lost or stolen cards should be reported within twenty-four (24) hours to either the Campus ID Services Office or to the Campus Public Safety Office. Individuals may also log into their GET Account and deactivate the card immediately. If an individual fails to deactivate through GET or notify ID Services/Public Safety concerning a lost or stolen ID Card, that individual is liable for the unauthorized charges to the account until notice is given.

III. Card Reader System.

Card reader door access will be issued to those individuals who require access to card reader equipped buildings and areas after normal operating hours and/or while buildings are secured. The *Door Access Authorization* form requires written approval by the dean, chairperson, or department head of the space or building involved before the requested card authorization is initiated. Individual users of the card reader system are charged with insuring that the ID card entrusted to them is always safeguarded. Persons loaning or otherwise misusing the card will be subject to disciplinary action.

IV. Key Control.

Individual users of the key control system are charged with insuring that the key entrusted to them is always safeguarded. Persons loaning or otherwise misusing the key will be subject to disciplinary action. Only one key will be issued per request form. Multiple keys will not be issued in the name of one individual for the purpose of passing them out to other individuals. Persons signing out keys are responsible for all keys signed out in their name. Keys shall not be held in a department without proper transfer to an individual. Exterior door keys to buildings equipped with card readers are limited by this policy. All others requiring after-hours access to buildings will utilize the card reader system or call Public Safety to gain access.

It is the department's responsibility to keep records of keys issued to their employees and to see that employees follow proper procedures in returning keys to Facilities Administration upon termination or transfer. A fee determined by the current Facilities Services replacement rate will be levied for replacement of lost keys, for each key that is not returned, or for which proper accounting has not been made. Any required building re-keying will be at the cost of the department responsible for the lost or stolen key.

A. Grand Master Key.

Authority to hold a Grand Master key to all locks of the system must be authorized by the COO or their designee.

A Grand Master Key will only be issued after a criminal background check is complete and if the individual has no felony convictions.

B. Master key or Sub-master Key.

Authority to hold a master key or sub-master key for all of a building or all of a system segment will be limited to the Provost, deans, chairpersons, department heads, building coordinators, and directors who have an entire building or system segment under their control. This authorization may be extended only to one other authorized delegate in a department.

Authority to hold Sub-Master keys for parts of a building or parts of a system segment will be limited to the following individuals:

i. Chairpersons, department heads, directors, faculty, graduate students, building coordinators, and technicians designated by department heads as requiring special afterhours access; and
ii. Custodial and maintenance personnel who have a continuing "need to enter" when occupants are not available to let them in.

V. Lock Removal.

Requests to have Locks removed from the university master lock system are submitted to facilities administration and must be approved by the COO or designee.

Authority: T.C.A. § 49-8-203

Previous Policy:

Defined Terms

Defined terms have a specific meaning within the context of this policy

Access Control:	Refers to keys, digital cards, and near field devices used to activate/deactivate locking mechanisms.
Least Privilege:	Limits users' access to only what is needed to do their jobs.
Locks:	Refer to mechanical lock and key devices and/or electronically controlled entry devices.

Policy History

Effective Date:

Revision Date:

Procedure

ETSU physical security includes all main campus buildings, offsite locations, athletic facilities, and any other facility under the care and control of ETSU.

I. Guest Access.

Guest access may be provisioned commensurate with necessity based on review and approval by the dean, chairperson, or department head of the space or building involved.

II. Contractor Access.

Guest access may be provisioned commensurate with necessity based on review and approval by the facilities administration.

III. Identification Card.

Deans, chairpersons, department heads, and directors having approval authority for issuance of access control/ID cards and keys, will ensure that proper controls and safeguards are maintained to protect the integrity of the security card reader access system and the security of ETSU facilities and activities. They will likewise ensure that card reader access authorization and key authorizations are limited to those individuals within their activity who have an official need.

Identification Card/Card Reader Applications are initiated and processed as follows:

A. Staff and faculty go to ID services to secure their ID after they receive their E number. Students go to ID services to secure their ID after they register for classes.

B. For other academic personnel not processed through Human Resources, the academic department provides ID Services a copy of the appointment letter or written verification of appointment. The completed application is forwarded to ID Services for issuance of the ID card. Applications for residents and fellows are completed by the respective dean's office at the time of appointment. The completed application is forwarded to ID Services for issue of the ID card. The Student Life Office issues applications for new or special students at the time of registration. For visitors who will be on campus several days and who will not be accompanied by University personnel (auditors, site visitors, etc.), the host unit provides to ID Services and Campus Police, in writing, details of the visit and will schedule issuance of ID(s) if required.

III. Card Reader System.

After a written request is submitted, the applicable dean, chairperson, department head, and director

or their designee approves or disapproves the request for card reader access for buildings and areas under their immediate control. Once an approval is received, a card is issued to the applicable user.

IV. Key Control.

A. Issuing a Key.

Keys are issued by facilities administration upon receipt of an approved key control request form. Key control request forms are available on the ETSU Facilities website under Useful Forms. The following guidelines apply to issuing a key:

i. All requests will be evaluated on the individuals need to enter a facility on a recurring basis.

ii. Key request authorizations need a dean, independent department head, department chairperson, director, or their designee signature. The delegation of this authority is limited to personnel under the direct budget and operational control of the individual doing the delegating. Designees may sign authorizations for interior door keys only.

B. Changing Key Assignment.

The changing of key assignments from one employee to another will be accomplished in the following manner:

i. The key is returned to the facilities administration where the signature of accountability is canceled, and a receipt issued.
ii. The key is reissued to another employee following the procedure of issuing a new key.
iii. Keys must be reassigned or returned in order for the Office of Human Resources Employee Separation Form to be completed for the individual terminating.

C. Return of Key.

Upon separation of employment from the University, all faculty and staff will return all building and office keys for which they are responsible to the Facilities Administration Key Control Office. Departments initiate an Employee Separation Form which is also signed by facilities administration personnel indicating all keys have been accounted for.

When an employee begins leave for any disciplinary actions, keys will be relinquished to the Facilities Services Key Shop at the onset of the leave, and reassigned to the employee upon return to active status.

D. Loss of Key.

The loss (or discovery) of an ETSU key is reported immediately to Public Safety. The following additional procedures apply:

i. Public Safety files a written police report outlining the circumstances of the loss or discovery.
ii. The key assignee renders a written statement affirming that if the key is recovered, it will be returned.
iii. A replacement key is not be issued until the required written report cited above is received and approval is granted to issue a duplicate key.

E. Change of Keys or Lock.

Normally, all keys and lock cores should be changed, or at least evaluated for change, at intervals not exceeding five years. The condition of keys and cores, number of lost keys, current and planned use of space, security problems, and current and future security needs are some of the more crucial factors to be considered in deciding when keys and cores should be changed. Movement of a department into space previously occupied by another usually justifies changing keys and lock cores at the time the move is made.

Lock change requests are submitted to Facilities Administration, outlining the building, space, and doors where changes are desired, and the reasons for change.

F. Upgrade of Security.

When a higher degree of security for funds, drugs, records, etc., is needed, facilities administration is notified, and assistance will be provided in determining the level of security needed. Proper forms authorizing entry to these areas are required, and it is imperative that the number of keys issued be restricted to the absolute minimum essential to the operation.

Procedure History

Effective Date:

Revision Date:

Related Form(s)

https://www.etsu.edu/students/idservices/docsandforms.php
https://www.etsu.edu/facilities/documents/key-control-order.docx

Scope and Applicability

Primary:

Secondary:

EAST TENNESSEE STATE UNIVERSITY

FIRE PROTECTION AND LIFE SAFETY POLICY	
Responsible Official: Chief Operations Officer	**Responsible Office:** Environmental Health and Safety

Policy Purpose

This policy specifies the program and procedures implemented to create a safe environment for East Tennessee State University (ETSU or University) faculty, staff, students, and visitors by applying recognized fire protection and life safety standards to everyday University operations.

Policy Statement

The purpose of this policy is to protect human life, property, and the environment from the risk of fire-related hazards through the application of federal and industry standards, regulations, best practices, engineering analysis, fire prevention techniques, and public fire safety education and awareness for the ETSU campus community.

The ETSU Office of Environmental Health and Safety (EHS) shall establish written procedures and processes for a fire and life safety inspection and preventative maintenance program which shall consist of:

1. Clearly defined roles, responsibilities, and accountability at all levels;
2. Aggressive risk assessment and management;
3. Preventative maintenance of all University fire and life safety systems;
4. Periodic physical inspections of all fire protection and life safety systems and equipment in all University facilities;
5. Detailed written follow-up reports outlining any system and/or equipment deficiencies and recommended actions to ensure functionality and compliance;
6. Maintenance and repair of fire and life safety systems and/or equipment that are expired or show signs of corrosion; and
7. Delivery of fire and life safety training and education.

Authority: The Focus Act, TCA § 49-8-203, et. seq; 29 CFR 1910.39(b); The Clery Act; NFPA

Defined Terms

A defined term has a special meaning within the context of this policy.

Policy History

Effective Date:

Revision Date: 03/04/23

Previous Policy Implemented December 2014

Procedure

Fire Protection and Life Safety Inspections

Effective Date:

Revision Date: 03/04/23

Related Form(s)/Links/Contacts

EHS Fire and Life Safety resources page

Annual Clery Fire Safety Report

29 CFR 1910.39(b)

- Housing and Residence Life (423) 439-4446
- Fire Protection Manager (Office of EHS) (423) 439-7773
- Facilities Services (423) 439-7900

Scope and Applicability

Primary:

Secondary:

GENERAL PURCHASING POLICY	
Responsible Official: **Chief Financial Officer**	Responsible Offices: **Tax and Revenue Services**

Policy Purpose

East Tennessee State University (ETSU or University) is required by state and federal law to establish and maintain a system of internal control. This policy specifies procedures for obtaining goods and services.

Policy Statement

This policy governs the purchasing process. For questions about the purchasing process you should contact the Procurement and Contracts Office.

I. Principles

A. All purchases must comply with this policy and the laws of the State of Tennessee for the purchase of goods and services.
B. The purchase must support the mission and purpose of the University.
C. The purchase must not be personal in nature.
D. The amount expended should be reasonable.
E. Employees of the University serve the interests of the State of Tennessee and must comply with the Conflicts of Interest and Commitment Policy.
F. The President of the University has delegated authority to the Associate Vice President for Tax and Revenue Services and the Manager/Director of Procurement and Contracts to make purchase commitments. The President of the University has delegated authority to the Associate Vice President for Tax and Revenue Services and the Manager/Director of Procurement and Contracts to sign contracts for the University when they are associated with purchase orders. No employee has authority to make any purchase commitment, enter into any contract for goods or services, or otherwise act with respect to third parties which may be construed as financially binding to the University except through the authority of Tax and Revenue Services, unless specifically authorized by other applicable University policy or in writing by the President. This policy applies to all expenditures of funds administered by the University, regardless of origin. This policy does not apply to agency funds set up with ETSU Financial Services.

G. The ETSU Standard Bid Terms and Conditions and the ETSU Code of Ethics in Procurement and Contracting (See Section VI, infra) are adopted as minimum standards in the procurement of goods and services.

H. Except as specifically provided in other University policies and guidelines, authority pursuant to those policies shall not include the purchase or lease of real property, the purchase of insurance, or purchases for capital outlay projects from any fund source whatsoever.

I. No employee of the University responsible for initiating or approving requisitions shall accept or receive, directly or indirectly, from any person, firm or corporation to whom any contract may be awarded, by rebate, gift or otherwise, any money or anything of value whatsoever, or any promise, obligation or contract for future awards or compensation. Whenever any contract/purchase order is awarded contrary to this provision, the contract/purchase order shall be void and of no effect, and if the violation was intentional, the employee responsible for the purchase shall be liable for any state funds paid contrary to this provision.

II. Purchasing

A. Planning a Purchase: In preparation of the purchase of goods and services, a clear description of the requirements or specifications is the basis for assuring that departmental needs will be met. The approving authority from the ordering department must assure that funds have been appropriated and are available for the purchase of materials, supplies, equipment or services prior to award of a contract. The ordering department is responsible for determining that all items to be purchased are necessary.

B. Purchase Requisition Procedures: Purchase requisitions should be submitted online by accessing the University purchasing system. Purchase requisitions are submitted by the ordering department, approved by the appropriate officials and forwarded electronically to the Procurement and Contracts Office for processing into a bid or a purchase order.

C. The purchase requisition should include, but is not limited to the following:

1. Information describing the purpose of the acquisition, technical requirements, bidder qualifications, and any other information considered relevant to the goods or services being acquired. Whenever possible, all specifications for materials, supplies, equipment and services shall be worded or designed so as to permit open and competitive bidding;
2. The quantity or number of articles or services required; and
3. The estimated cost of goods or services.

D. Additional Purchasing Methods: In addition to the purchase requisition, other purchasing methods, such as the Procard and contract purchases may be available.
E. Competitive Bidding and Specifications: All purchases valued at $25,000 or more shall be based upon the principles of competitive bidding except as provided herein. The unit of analysis for application of the bidding threshold is the individual invoice, receipt, purchase order, estimate, etc. Primary responsibility for determining a single purchase is with the department. The Procurement and Contracts Office shall review purchases to ensure compliance with this Policy. Departments shall not intentionally divide invoices, receipts, purchase orders or estimates to stay below the $25,000 threshold.
F. Whenever possible, all specifications for materials, supplies, equipment and services shall be worded or designed so as to permit open and competitive bidding for the supplying of the articles, commodities or services to which they apply.
G. Bidding is required when the total purchase amount is $25,000 or more. A minimum of three bids is required when the total purchase amount is $25,000 to $100,000. Departmental personnel may contact sources of supply for quotes when the amount of the total purchase is $25,000 or more but less than $100,000. The Procurement and Contracts Office will assist in the development of specifications and provide capable suppliers upon request. The Procurement and Contracts Office is also available to obtain the bids. All bid information is to be attached as internal information on the purchase requisition in the University purchasing system. If available, furnish with the purchase requisition such specifications, catalog pages, brochures, or other data as will provide an adequate basis for determining the quality and functional capabilities of the products being requested.
H. The Procurement and Contracts Office will issue bids for goods and services $100,000 or more. Exceptions to this are construction contracts in which the Office of Facilities Management as the State Procurement Agent will route any construction contracts over $100,000 to the Office of State Architect for approval. These contracts must be approved and signed by the President, University Counsel, and the Chief Financial Officer.
I. The University shall actively solicit bids from small, minority, service-disabled veteran, and woman-owned businesses in order to obtain a fair proportion of goods and services from such businesses, whenever possible.
J. Non-Competitive Purchases: Goods and services over the bid threshold may be procured without competitive bidding only if such purchases are justified in writing and approved by the President, Associate Vice President for Tax and Revenue Services, or Manager/Director of Procurement and Contracts.
K. Emergency Purchases: Requests for purchases of specific materials, supplies, equipment, or services may be made in the open market for immediate delivery only to meet bona fide emergencies arising from any unforeseen cause. The President must approve all bona fide emergency purchase requests of $750,000 or more. The Chief Operating Officer must approve all emergency purchases less than $750,000. A written report on the circumstances of any such emergency justifying the purchase shall be prepared by the ordering department and maintained by the

University. All emergency purchases shall, if practicable, be made on the basis of competitive bids.

L. Contracts and Agreements: All contracts and agreements will be in conformance with ETSU policy on Contracts and Signature Authority and other State requirements.

M. Fiscal Review: Certain procurements/contracts require approval by the Board of Trustees or the Board's designee, and the State of Tennessee Fiscal Review Committee. (Allow a minimum of 75 days prior to the effective date of the procurement agreement). This includes procurements/contracts that:

1. Are non-competitive;
1. Are or have the potential of being for a period of more than one year; and
2. Exceed $250,000 in total value (including all potential renewals)

N. Advanced Fiscal Review Exemptions: The State of Tennessee Fiscal Review Committee has established that certain categories of contracts and amendments entered into by higher education institutions are exempt from advanced fiscal review but, instead, must be reported to the State of Tennessee Fiscal Review Committee on a quarterly basis. The ETSU Office of Procurement and Contract Services shall maintain a list of and report any such exemptions to the State of Tennessee Fiscal Review Committee on a quarterly basis.

O. Prohibited Transactions: No personal items shall be purchased through the University or from funds of the University for any employee of the University or any relative of any employee. Personal gifts for employees cannot be purchased with university funds. Whenever any contract/purchase order is awarded contrary to this provision, the contract/purchase order shall be void and of no effect, and if the violation was intentional, the employee responsible for the purchase shall be liable for any state funds paid contrary to this provision.

P. Any software that stores, processes, or transmits university data or integrates with university information systems needs to be reviewed and approved by Information Technology Services.

III. Special Purchasing Considerations

A. Business Meals: The University may pay or reimburse properly documented meals when the primary purpose is a business discussion. Business meals generally include at least one non-university employee. However, occasional gatherings of University employees may also be reimbursed as business meals. Expenses may be incurred only for those individuals whose presence is necessary to the business discussion.

B. In addition to an itemized receipt, IRS rules on substantiation of business expenses require documentation of the time, date, place, specific topic of discussion and attendees at the meals. The documentation requirements apply to all on-campus or off-campus business meals, regardless of payment methods. Accordingly, all on-campus dining facilities require this documentation for all meals charged to

departmental accounts.

C. Under no circumstances will alcohol expenditures be reimbursed. The University will deny reimbursement for meal expenses that lack documentation or a clear business purpose. Gatherings that are primarily social in nature do not qualify for payment or reimbursement as business meals.
D. Faculty/Staff Recognition Events: Institutional funds may be used to purchase food and non-alcoholic beverages for recognition, appreciation and/or retirement events. Expenses for these events must be reasonable. Recognition gifts and retirement plaques are allowable up to a reasonable value limit per employee/retiree recognized.

IV. Examples of Purchases Not Allowed with University Funds

A. Gifts and flowers except for officially sponsored events and student activities
B. Personal purchases for employees or students
    1 Professional license fees include any Tennessee State Health Professional Board, or other state or national professional board licenses
    2. Memberships, Dues and Subscriptions: including any personal membership, dues, or subscriptions in the name of the individual, any civic organizations, or professional organizations in the name of an individual. To be allowed the fee has to be an Institutional fee in the name of ETSU, a college, or a department, not an individual.
    3. Purchases for office use: including decorations for private offices, coffee pots, microwaves, tissues, food, drinks, cups, plates, etc.
C. Employee monetary awards/rewards including cash, gift cards or gift certificates: Employee awards are provided using processes established in the Foundation and are paid through Payroll as extra compensation.

V. Permitted Transactions for Non-Employees with University Funds

A. Honoraria.
B. Token of appreciation for service rendered: $50 or less per person.
C. Incentives/Rewards for participating in research studies, surveys, or projects, or for attending events.
D. Promotional items for give-away in order to promote departments and departmental programs.
E. Gift cards are allowed to be purchased for payment to research participants only. Non-employee and non-resident alien research participant payments are limited to a maximum of $50 per payment and a total payment of less than $600 to any one research participant. The department must retain a copy of the research participant name, address, social security number and signature acknowledging receipt of the gift card. The Department must be able to show that all the gift cards were

distributed. These records are subject to audit by the university and state. A request to purchase gift cards should be sent to Accounts Payable for a check to be issued to the vendor. University Procards cannot be used to purchase gift cards.

F. Cash payments: Cash payments are allowed for research participants only. Non-employee and non-resident alien research participant payments are limited to a maximum of $50 per payment and a total payment of less than $600 to any one research participant. Any individual research participant payment over $50 must be processed through Accounts Payable via a check to the individual research participant. Complete the Cash Payment to Research Participants form and return it to Financial Services before any funds can be distributed. Research participant name, social security number, address and signature acknowledging receipt of the cash must be obtained. Differing from the use of gift cards, the petty cash receipts are returned to the Bursar's Office when the petty cash account is closed out at the end of a grant or when the fund is replenished. The receipts are retained in the Bursar's vault and are subject to audit by university and the state. Note: Whether gift cards or cash are distributed, a method of securing cards or cash is needed.

VI. Code of Ethics in Procurement and Contracting

The code of ethics was developed by East Tennessee State University, approved by the Board of Trustees, and shall be applicable to all ETSU employees who are primarily responsible for the purchase of goods or services for the institution.

A. Statement of Policy
   1. Employees must discharge their duties and responsibilities fairly and impartially.
   2. They also should maintain a standard of conduct that will inspire public confidence in the integrity of the institution.

B. General Standards of Ethical Conduct

   1. Any attempt to realize personal gain through public employment, inconsistent with the responsible discharge of that public employment, is a breach of public trust.
   2. Employees shall base all purchases on the principle of competitive bidding consistent with policies of the Board and the institution.
   3. Employees shall grant all competitive bids equal consideration, regard each transaction on its own merits, and foster and promote fair, ethical, and legal trade practices.
   4. Employees shall not engage in bid-splitting by intentionally dividing orders for supplies and equipment into smaller quantities to avoid policy thresholds.
   5. Employees shall avoid misrepresentation and deceitful practices, and demand honesty in sales representations whether offered through the

medium of a verbal or written statement, an advertisement, or a sample of a product.

6. Employees shall be receptive to competent counsel from colleagues, and be willing to submit any major controversy through the appropriate appeals processes.
7. Employees shall accord prompt and courteous reception insofar as conditions permit to all who call on legitimate business missions.
8. Employees shall not use without consent the original designs developed by a vendor for competitive purposes.

C. Conflict of Interest

1. It shall be a breach of ethical standards for any employee, in the performance of the employee's official duties, to participate directly or indirectly in any proceeding or application, request for ruling or other determination, claim or controversy, or other particular matter pertaining to any contract, or subcontract, and any solicitation or proposal thereof, in which to the employees' knowledge:
    a. the employee or any member of their immediate family has a substantial financial interest; or
    b. a business or organization in which the employee or any member of their immediate family has a substantial financial interest as an officer, director, trustee, partner, or employee, is a party; or
    c. any other person, business, or organization with whom the employee or a member of their immediate family is negotiating or has an agreement concerning prospective employment is a party.
2. Direct or indirect participation shall include but not be limited to involvement through decision, approval, disapproval, recommendation, preparation of any part of a purchase request, influencing the content of any specification or purchase standard, rendering of advice, investigation, auditing or in any other advisory capacity.

D. Gratuities

It shall be a breach of ethical standards for any employee or former employee to solicit, demand, accept, or agree to accept from another person, a gratuity or an offer of employment, in connection with any decision, approval, disapproval, recommendation, preparation of any part of a purchase request, influencing the content of any specification or purchase standard, rendering of advice, investigation, auditing, or in any other advisory capacity in any proceeding or application, request for ruling or other determination, claim or controversy, or

other particular matter, pertaining to any contract or subcontract and any solicitation or proposal thereof.

E. Contemporaneous Employment Prohibited

It shall be a breach of ethical standards for any employee who is involved in procurement to become or be, while such an employee, the employee of any party contracting with the particular governmental body by which the employee is employed.

Defined Terms

A defined term has a special meaning within the context of this policy.

CONFLICT OF INTEREST:	A conflict of interest occurs when the personal interests, financial or otherwise, of a person who owes a duty to the Board of Trustees or the University (all employees) actually or potentially diverge with the person's professional obligations to and the best interests of the Board of Trustees and University. It is a conflict of interest for any person or any company with whom such person is an officer, a director, or an equity owner of greater than 1% interest to bid on any public contract for products or services for a governmental entity if such person or a relative of such person is a member of a board or commission having responsibility for letting or approving such contract. For purposes of this section only, "relative" means spouse, parent, sibling, or child. It is the policy of the University that no employee shall use their employment for personal benefit. Any appearance of favoritism or influence in doing business is prohibited.
MINORITY-OWNED BUSINESS:	A continuing, independent, for-profit business which performs a commercially useful function and is at least 51% owned and controlled by one or more minority individuals who are impeded from normal entry into the economic mainstream because of past practices of discrimination based on race or ethnic background.

NON-COMPETITIVE PURCHASES AND CONTRACTS:	Purchases and contracts made when items or services are unique and possess specific characteristics that can be filled by only one source.
PROCARD:	The procurement card program available for purchases of goods less than $5,000.
SERVICE DISABLED VETERAN BUSINESS:	Tennessee service-disabled veteran means any person who served honorably on active duty in the Armed Forces of the United States with at least a twenty percent (20%) disability that is service-connected meaning that such disability was incurred or aggravated in the line of duty in the active military, naval or air service. "Tennessee service disabled veteran owned business" means a service disabled veteran owned business that is a continuing, independent, for profit business located in the state of Tennessee that performs a commercially useful function, and is at least 51% owned and controlled by one (1) or more service-disabled veterans.
SMALL BUSINESS:	A business which is independently owned and operated and is not dominant in its field of operation.
SURPLUS PROPERTY:	Any University property such as movable equipment or supplies (not real property such as land or buildings) a department determines to be excess to its needs and for which the department has no foreseeable requirement.
UNLAWFUL EMPLOYEE ACTIVITIES:	It is unlawful for any employee to bid on, sell, or offer for sale, any merchandise, equipment or material, or similar commodity, to the state of Tennessee or to have any interest in the selling of the same to the state during that person's term of employment and for six months thereafter (T.C.A. § 12-4-103). Disclosure of any such transaction by an employee or member of the employee's family or by a business in which an employee or member of the employee's family has any significant (more than 4%) ownership interest or for which an employee or employee

	family member serves as an officer is required by this policy. Family member includes the spouse and children (both dependent and non-dependent) of a person covered by this policy.
WOMAN-OWNED BUSINESS:	A woman-owned business that is a continuing, independent, for-profit business which performs a commercially useful function, and is at least 51% owned and controlled by one or more women; or, in the case of any publicly owned business, at least 51% of the stock of which is owned and controlled by one or more women and whose management and daily business operations are under the control of one or more women.

Authority: T.C.A. § 49-8-203, et. Seq; T.C.A. § 9-2-102; T.C.A. § 9-18-102(a); Standards for Internal Control in the Federal Government (Green Book) GAO-14-704G

Policy History

Effective Date:

Revision Date: 3/23/2023

Procedure (s)

Procedure History

Scope and Applicability

Check those that apply to this policy and identify proposed sub-category.

	Governance	
	Academic	
	Students	
	Employment	
	Information Technology	
	Health and Safety	
X	Business and Finance	
	Operations and Facilities	

	Communications & Marketing	
	Advancement	

EAST TENNESSEE STATE UNIVERSITY

HAZARDOUS ENERGY CONTROL (LOCKOUT/TAG-OUT)	
Responsible Official: Chief Operations Officer	**Responsible Office:** Environmental Health and Safety

Policy Purpose

This policy specifies the procedures for implementing the federal Occupational Safety and Health Administration (OSHA) Standard for the Control of Hazardous Energy (Lockout/Tagout), 29 CFR 1910.147.

Policy Statement

East Tennessee State University (ETSU) is committed to providing a safe and healthy work environment for the campus community. This policy is intended to protect ETSU employees, students, visitors, and other members of the campus community from injury due to the unexpected energizing, start-up, or release of stored energy during the servicing and maintenance of machines, equipment, or systems.

All machines, equipment, and systems that fall within the scope of this policy must be locked-out or tagged-out by authorized employees, in accordance with the ETSU Office of Environmental Health and Safety's (EHS) written energy control procedures. All outside contractors working on or at the premises of ETSU will be required to follow substantively similar, OSHA-compliant, procedures.

No ETSU employee, student, or contractor shall attempt to start, energize, or use any machinery, equipment, or system that has been locked-out or tagged-out for servicing or maintenance. The servicing or maintenance of machines, equipment, and systems is solely under the jurisdiction of Facilities Management (or contractors they hire) at ETSU.

This policy applies to all ETSU employees, students, contractors, and others who are exposed to, work with, or supervise operations involving work with hazardous energies on the ETSU campus and its facilities.

Authority: The Focus Act, TCA § 49-8-203, et. seq; Occupational Safety and Health Administration OSHA 29 CFR 1910.147

Previous Policy Implemented December 2014

Defined Terms

A defined term has a special meaning within the context of this policy.

Policy History

Effective Date:

Revision Date: 03/04/23

Procedure

Environmental Health and Safety Lockout/Tagout procedures.

Effective Date:

Revision Date: 03/04/23

Related Form(s)/Links

OSHA Standard 1910.147

Anyone having questions may contact the Office of Environmental Health and Safety (423) 439-7784.

Scope and Applicability

Primary:

Secondary:

EAST TENNESSEE STATE UNIVERSITY

MEMORANDUM

TO: University Council

FROM: Christina A. Graham, Chief Financial Officer for Business and Finance; Myra Jones, Associate Chief Information Officer/ITS Chief of Staff; Dr. Mark Jee, Director of Environmental Health and Safety; Jeremy Ross, Chief Operating Officer; Kay Lennon McGrew, Esq., Associate University Counsel and Policy Counsel; Harden Scragg, Esq., Staff Attorney and Assistant Policy Counsel

DATE: June 1, 2023

RE: Consent Agenda Policy Items for June 12, 2023 UC Meeting

- *General Purchasing Policy*
- *Hazardous Energy Control* (*Lockout/Tagout*)
- *Acceptable Use of Information Technology Resources*
- *Building Access Control Policy*
- *Fire Protection and Life Safety Policy*

I. General Purchasing Policy.

A. Introduction.

This policy governs the purchasing process and specifies the procedures for obtaining goods and services. It contains two major revisions.

Policy revisions include:

1. Subpart II (G and H) modifies the formal bid threshold from $75,000 to $100,000; and
2. A new subpart Sub-part II (P) has been added to the General Purchasing section to reflect the approval needed by ITS for all software products.

This policy will be effective 07/01/2023 (Fiscal Year 2024).

A copy of the policy is attached.

B. Legal Review.

The Office of University Counsel completed its review of this policy on 04/28/2023. Counsel found no legal issues and no conflicts or inconsistencies with other ETSU policies or procedures.

C. Public Comment Period.

The policy was posted from for public comment from 4/18/2023 to 5/01/2023. Two comments were submitted during this period:

Comment from Richard Prince: *"The language in sub-part II P is much too restrictive for the needs of faculty, researchers, and the university as a whole. Nearly any purchase going forward will include an aspect of software that will interface with the university network. Giving ITS the final say in a purchase is inappropriate given the teaching and research missions of the university."*

Sponsor's Response: ITS provides the highest quality technology services to students, faculty, and staff and delivers technologies that advance the University's academic, research, and administrative goals. The university has a legal obligation to protect the privacy and security of university data and systems. It is essential to involve ITS in the review and approval of new software that will interface with university IT assets to ensure the software is both secure and compatible. The General Purchasing Policy as written captures this necessary process.

Comment from Jessimine Strauss: *"II Purchasing G appears to be missing a ["or more"] in relation to the third $25,000. Currently reads as equal to exactly $25,000 and also less than $100,000. [It should clarify $25,000 or more]"*

Sponsor's Response: Purchasing provision II (G) has been revised accordingly to clarify the purchasing language.

D. Recommendation.

IN CONSIDERATION of all of the above the Office of University Counsel recommends **APPROVAL** of the **General Purchasing Policy.**

II. Hazardous Energy Control (Lockout/Tagout).

A. Introduction.

This policy specifies the procedures for implementing the federal Occupational Safety and Health Administration (OSHA) Standard for the Control of Hazardous Energy (Lockout/Tagout), 29 CFR 1910.147.

A copy of the policy is attached.

B. Legal Review

The Office of University Counsel completed its review of this policy on 04/07/2023. Counsel found no legal issues and no conflicts or inconsistencies with other ETSU policies or procedures.

C. Public Comment Period.

The policy was posted from for public comment from 4/5/2023 to 4/18/2023. No. comments were received.

D. Recommendation

IN CONSIDERATION of all of the above, the Office of University Counsel recommends **APPROVAL** of the policy on **Hazardous Energy Control (Lockout/Tagout).**

III. Acceptable Use of Information Technology Resources.

A. Introduction.

This policy provides a framework for the appropriate and respectful use of information technology resources. The policy is intended to prevent abuse of resources and to ensure that usage honors the public trust and supports the University's mission.

A copy of the policy is attached.

B. Legal Review.

The Office of University Counsel completed its review of this policy on 04/06/23. Counsel found no legal issues and no conflicts or inconsistencies with other ETSU policies or procedures.

C. Public Comment Period.

The policy was posted from for public comment from 04/05/2023 to 04/18/2023. No comments were received.

D. Recommendation.

IN CONSIDERATION of all of the above, the Office of University Counsel recommends **APPROVAL** of the policy on **Acceptable Use of Information Technology Resources.**

IV. Building Access Control Policy.

A. Introduction.

This policy specifies when and how access control devices, electronic and/or key access is granted to ETSU facilities. ETSU will control access to facilities based on need, required job responsibilities, individual accountability, and least privilege.

A copy of the policy is attached.

B. Legal Review.

The Office of University Counsel completed its review of this policy on 03/29/2023. Counsel found no legal issues and no conflicts or inconsistencies with other ETSU policies or procedures.

C. Public Comment Period.

The policy was posted from for public comment from 04/05/2023 to 04/19/2023. Two comments were received:

Comment from Brian Thompson:

> "*1. Policy Section II. If students who live in on-campus housing withdrawal from the university, their ID is needed to move out of their building. Student housing staff are the ones who check these students out after they remove personal belongings from their rooms. The checkout process involves removing encoding from the ID. I'd recommend establishing a protocol for how the ID is turned back in to the University. Does this have to occur during business hours at ID Services? Are Housing staff responsible for collecting the ID when said student checks out of their residence hall or apartment room? If so, where are those IDs turned in and when? What kind of enforcement is in place for those who do not turn in their ID upon withdrawal from the University?*
>
> *Students do not always report their ID lost or misplaced promptly. If reported to housing staff after hours, staff do call Public Safety. If during office hours, housing staff does contact me, who can disable the ID due to my position.*

Sponsor's Response: After consultation with ID services, ID's will be deactivated rather than returned. The policy has been updated to reflect this change.

Comment from Amy Slaughter: "Students who withdrawal have never returned their ID card. I am unsure of how this would be enforced. There is also not a graduation date or expiration date on the ID card. Those dates are automated by Banner and placed into CBORD behind the scenes. The cost of reprinting each time someone changes their graduation date would be way too high. The word fail in the last sentence should also be plural.
Policy Statement Section III

Reword the second sentence, the words from/must are not making sense. There is not an application for the ID card, as most people already have one. Access can be applied to a card once approved.

Procedure Section II

Reword: issuance of ID access control and keys. This will ensure that proper
Staff/faculty receive ID cards after E# is received. Students receive ID cards after they have registered for classes.
Not sure if the host unit has ever provided details of the visit to both ID and public safety. How detailed does this need to be? Usually just a general memo is sent to ID.

Procedure Section III

Once an approval is received, the access is issued to the applicable user. (card should already be made at this point)

Sponsor's Response: After consultation with ID services, ID's will be deactivated rather than returned. The policy has been updated to reflect this change. The policy was updated to reflect to process by which students receive their ID's. Information disclosed by host units is done through a form that is already in use. This is not a new process.

D. Recommendation.

IN CONSIDERATION of all of the above, the Office of University Counsel recommends **APPROVAL** of the **Building Access Control Policy.**

V. Fire Protection and Life Safety Policy.

A. Introduction.

The purpose of this policy is to protect human life, property, and the environment from the risk of fire-related hazards through the application of regulations, best practices, engineering analysis, fire prevention techniques, and public fire safety education and awareness for the ETSU campus community.

A copy of the policy is attached.

B. Legal Review.

The Office of University Counsel completed its review of this policy on 04/23/23. Counsel found no legal issues and no conflicts or inconsistencies with other ETSU policies or procedures.

C. Public Comment Period.

The policy was posted from for public comment from 05/16/2023 to 05/29/2023. One comment was received during this period:

> *Comment from Susan Epps:* "*It seems like the purpose of the policy is to establish the elements that are to be included in the fire and life safety inspection and preventative maintenance program, (not to protect life, etc.).*"

Sponsor's Response:

The purpose of specifying the elements that are to be included in the fire and life safety inspection and preventative maintenance program is to protect human life, property, and the environment from the risk of fire-related hazards through the application of federal and NFPA regulations, best practices, engineering analysis, fire prevention techniques, and public fire safety education and awareness for the ETSU campus community.

.

D. Recommendation.

IN CONSIDERATION of all of the above, the Office of Environmental Health and Safety recommends **APPROVAL** of the policy on **Fire Protection and Life Safety Policy**