

Management Assessment Tool (MAT)
Last revised 08/11/11

Note to Mac Users:

In order for the links to function correctly, you must open in Adobe Reader or Professional - Not in Preview

As someone with administrative or supervisory responsibilities, you have a stewardship responsibility to support and enhance the mission of UTSA, to ensure that the University fulfills its legal and financial obligations to internal and external stakeholders, to safeguard the University's financial, human, information and physical assets, and to create an atmosphere that encourages all members of the University community to contribute to the overall excellence of the University. The MAT has been designed to assist administrators/managers with the annual certification process.

[Overview](#)
 [Fiscal Management](#)
 [Purchasing](#)
 [Historically Underutilized Business \(HUB\)](#)
[Business Services Contracts and Leases](#)
[Capital Assets Management](#)
[Gifts](#)
[Human resources](#)
[Equal Employment Opportunity Compliance](#)
[Environmental Health and Safety](#)
[University Police](#)
[Key and Card Access](#)
[Emergency Preparedness](#)
[Information Technology](#)

OVERVIEW		
STATEMENT/QUESTION	RESOURCES	BEST PRACTICES/SUGGESTIONS
1. All employees paid from accounts for which I am the Account Administrator (my Accounts) have completed their required compliance training (ACK2010).	The Learning Source HOP 9.40 - General Compliance Training	<ul style="list-style-type: none"> Emphasize to all employees the importance of completing online compliance training. Employees will be notified via email when training has been assigned and will be given a deadline to complete the training. Supervisors and Vice Presidents will be notified of non-completion. New employees will be assigned training within 30 days of hire. Existing employees are required to take annual refresher training in January of each year. Note: Effective January 2011, existing employees will be required to complete refresher training every other year, depending on employee's reporting structure. Student employees are required to take compliance training as well. It is important that email addresses in DEFINE are accurate so employees receive their training notifications.
2. I am aware and all employees paid from my Accounts (as applicable) have been informed that ethical or legal concerns raised by	UTSA Standards of Conduct Guide for Employees	<ul style="list-style-type: none"> Encourage employees to bring questions or observations of unethical activity to their supervisor. Supervisors should direct employees to the appropriate offices listed in the UTSA Standards of Conduct Guide for

<p>employees or students should always be taken seriously and should be referred to the appropriate office at UTSA for handling.</p>	<p>HOP 4.01 - Code of Ethics HOP 4.31 - Conflicts of Interest</p>	<p>Employees.</p> <ul style="list-style-type: none"> • Inform employees they can report suspected issues of non-compliance anonymously through the Compliance Hotline 1-877-888-0002 or via the web at https://www.tnwinc.com/webreport/. More information about the Hotline is available on the Office of Institutional Compliance & Risk Services Web site. • Ethical or legal concerns can be reported to the Chief Legal Officer (Legal Affairs) at 458-4105.
<p>3. I am aware that it is important to have measurable written goals and objectives for my area/department.</p>		<ul style="list-style-type: none"> • Define department/unit mission statement. • Develop long-term strategic goals. • Develop measurable annual goals based on your department's mission and strategic goals. • Create an action plan to achieve annual goals. • Communicate goals and action plan to all employees. • Evaluate action plan and goals annually. • Provide new employees with an orientation regarding their duties and responsibilities. An On-the-Job Orientation Checklist is available on the Human Resources Web site.
<p>4. I am aware that it is important to have written procedures for critical systems/processes in my area/department.</p>		<ul style="list-style-type: none"> • Identify critical operations. • Develop written procedures and review and update them annually.

FISCAL MANAGEMENT		
GENERAL		
<p>5. My area/department has a system for reconciling accounts on a monthly basis to determine whether the university's accounting records match my area/department's records. Procedures are in place to ensure appropriate action is taken in the event that errors and/or unauthorized transactions are identified, and all account reconciliations are dated and signed by the preparer and the reconciler.</p>	<p>Policy on the Annual Financial Report</p> <p>Online guidelines, forms, and training for Statement of Accounts reconciliation</p> <p>Management Responsibilities Guide</p>	<ul style="list-style-type: none"> • Managers should have a working knowledge of their budgets. Account information can be viewed from DEFINE and UT Direct. • Implement a departmental system for tracking and reviewing departmental expenditures and revenue. The type of system used may vary depending on the complexity of the department's accounts. Review the information provided on the Accounting Web site under Statement of Accounts. • If possible, assign different individuals the responsibility for entering data into the departmental system and the responsibility for reconciling the departmental system to DEFINE. • Check departmental reconciliations monthly and ensure all transactions are appropriate and there are no misstatements or omissions. • Ensure errors are corrected immediately. • If needed, attend training class on Understanding the Statement of Accounts (TXClass AM0506).
<p>6. My area/department is structured so one person does not create, approve, and reconcile transactions. If I do not have the</p>	<p>Fiscal Management Operational Guideline - Monitoring Plan for Segregation of</p>	<ul style="list-style-type: none"> • Proper segregation of duties in a department ensures no single individual handles all aspects of a transaction or business process, thus reducing the possibility of undetected errors or fraudulent activity.

<p>staff to adequately segregate these duties, I understand that as area/department head I must take a more active role in monitoring my area/department's accounts.</p>	<p>Duties and Reconciliation of Accounts</p> <p>Segregation of duties chart</p>	<ul style="list-style-type: none"> • Ensure no one person handles all phases of a transaction, e.g., creates, approves, and reconciles.
<p>7. There is a process in my area/department for reconciling cash and check income records to deposit documentation.</p> <p>Note: Areas/Departments accepting funds on behalf of UTSA must have an authorization request on file with the Office of Financial Services and University Bursar and all employees authorized to handle or accept currency, checks, or credit cards on behalf of UTSA must attend the Cash Handling 101 (AM560) training class.</p>	<p>Cash Handling Request Form</p> <p>Fiscal Management Operational Guidelines - - Cash Handling and Management and Processing Cash Payments</p> <p>UTS166 Cash Management and Cash Handling Policy</p>	<ul style="list-style-type: none"> • A department that receives cash and/or checks should have a system in place for recording those receipts, e.g., cash register or log. • Cash register tapes or logs should be compared to actual deposits on a routine basis to ensure all income is being deposited. • Income trends should be analyzed to determine whether actual income matches expected income. • A receipt book should be used for in person transactions. • Good segregation of duties is critical to prevent fraud in a cash operation. Having one person in charge of all phases of a cash operation is risky - the rule of thumb is there should be at least two sets of eyes on every transaction. Ideally you should ensure the individual responsible for record keeping (reconciling cash/checks received to cash register tapes, registration or other income records) is different from the person who has custody of the cash/checks (opens mail, prepares deposit). In small departments this can be a challenge, however, there are creative ways to compensate if you cannot fully segregate duties, e.g., have someone outside of the process analyze sales and deposits for reasonableness or monitor for unusual trends.
<p>8. Cash/checks are adequately secured at all times, access is restricted to the extent possible and checks are immediately endorsed when received.</p> <p>Note: Areas/Departments accepting funds on behalf of UTSA must have a security policy on file with the Office of Financial Services and University Bursar.</p>	<p>Departmental Cash Handling Security Policy</p> <p>Fiscal Management Operational Guidelines - - Processing Cash Payments</p> <p>UTS166 Cash Management and Cash Handling Policy</p>	<ul style="list-style-type: none"> • As a minimum requirement, keep cash/checks locked in drawer or safe at all times. • Establish accountability for cash/checks by limiting access to the key or combination to as few individuals as possible.
<p>9. Cash and checks received totaling \$500 or more are deposited with Fiscal Services within one business day and cash receipts under \$500 are deposited within a week.</p>	<p>UTS166 Cash Management and Cash Handling Policy</p> <p>Fiscal Management Operational Guidelines - - Cash Handling and Management and Processing Cash Payments</p>	<ul style="list-style-type: none"> • Depositing cash and checks timely is key to reducing the risk of theft and should be a priority when organizing employees' duties. • Deposits should be delivered to Fiscal Services in a tamper evident bag by two employees. • Note: Any deposit or combination of containing more than \$5000 in cash (currency and coin) <u>must</u> be secured in tamper evident bags and <u>must</u> have a UTSA Police escort when the deposit is delivered to Fiscal Services.
<p>10. Monthly phone charges are reviewed to ensure employees are not making personal long-distance calls on area/departmental phones and employee(s) who do so are</p>		<ul style="list-style-type: none"> • Inform staff that university phones should not be used for personal long distance calls. If personal long distance charges are incurred, the university should be reimbursed in a timely manner. • Review monthly phone bills and question unusual charges.

<p>required to reimburse UTSA the full amount including taxes.</p>		<ul style="list-style-type: none"> • Staff should review phone bills on a monthly basis and each staff member should attest phone calls are business related. • The electronic phone bills should be saved to a folder (e.g. by month) on a common network drive that can be accessed by all employees. • Employees may attest by email, and those emails should be saved to the folder on the common network drive.
--	--	---

PURCHASING		
<p>11. All employees who procure goods and services on my Accounts attend purchasing training prior to placing orders on the system.</p>	<p>Purchasing Office Web site</p>	<ul style="list-style-type: none"> • Managers should have a working knowledge of purchasing policies and procedures. • Employees are stewards of University funds; therefore, purchases must be business related and consistent with the department's mission. • If possible, to ensure proper segregation of duties, the person making purchases should not also reconcile the Statement of Accounts. • Ensure that employees who perform purchasing duties attend initial purchasing training (followed by subsequent refresher courses) within 30 days of starting employment. TXCLASS provides a number of training classes concerning purchasing procedures and the use of ProCards. TXCLASS can be accessed online through UTDirect or by calling HR Training and Development at 458-4658. • Emphasize the importance of following purchasing regulations. • Ensure supporting documentation is filed and maintained in accordance with the UTSA records retention schedule. http://www.utsa.edu/pds/records/forms/SLR105UTSA.pdf • Utilize the UTSA ProCard for purchases under \$5,000 when possible (items purchased must comply with ProCard regulations and restrictions). • Notify Purchasing immediately when discrepancies or problems occur with vendors or contractors. • Call Purchasing Buyers if you have questions. http://www.utsa.edu/purchasing/contact.cfm
<p>12. There is a process in my area/department to ensure the Purchasing Department handles all purchases over \$5,000 and I am aware and have informed all employees paid from my Accounts that orders cannot be split to avoid these dollar requirements.</p>	<p>Purchasing Office Web site</p>	<ul style="list-style-type: none"> • Maintain adequate supporting documentation for all purchases in the event of an audit or other requests for information. • Ensure employees who initiate and approve transactions are familiar with guidelines and restrictions for different accounts. • Expenditure transactions and related vouchers must be independently reviewed for completeness, accuracy, and compliance with University policies and in agreement with supporting documentation before being approved for payment. • Standardize specifications and requirements for commodities and services where possible.
<p>13. Central Receiving is notified immediately when goods are delivered directly to my area/department and to ensure goods are verified and Central Receiving is notified of</p>	<p>Central Receiving Web site</p>	<ul style="list-style-type: none"> • Ensure employees who receive goods in your department are aware they should notify Central Receiving immediately to ensure timely Vendor payments. Departments may incur monetary penalties under

<p>any discrepancies within 3 days. I am aware and have informed all employees paid from my Accounts that the area/department could be subject to interest penalties when vendors are not paid within 30 days.</p>		<p>the Prompt Payment Law if vendors are not paid within 30 days.</p> <ul style="list-style-type: none"> • If goods delivered to a department are damaged or are not what was ordered, the supplier should be contacted immediately. Central Receiving should be notified once the vendor has remedied the situation to your satisfaction so the vendor can be paid. • Ensure items are inspected and counted prior to signing and dating the receiving report/form from the vendor. • Departments should have a system for tracking outstanding purchase orders, e.g. an internal filing or accounting system.
<p>14. ProCard purchases on my Accounts comply with UTSA requirements and restrictions for using the ProCard.</p>	<p>UTSA ProCard Web site</p>	<ul style="list-style-type: none"> • Managers should have a working knowledge of ProCard policies and procedures. • Managers should be aware of items that cannot be purchased using the ProCard and should ensure cardholders are aware of these items as well. • ProCard restrictions can be viewed at: http://utsa.edu/pds/ProCard/restrictions.cfm • Ensure ProCard purchases are appropriate for the purposes/mission of the department/unit. • Maintain a log of ProCard purchases and retain adequate supporting documentation for all ProCard purchases, including Internet purchases, e.g. invoice, packing slip. • Suspicion of possible cardholder abuse of privileges should be reported to the Procard Office immediately. • Before approving the electronic voucher in DEFINE for ProCard purchases, review all transactions to ensure they are reasonable and appropriate for the department. Unusual transactions should be questioned. • Promote use of the ProCard for purchases made over the telephone or the Internet. • Call the ProCard office at 458-4059 if you have any questions or problems with the ProCard. • Ensure sales tax is not charged on ProCard transactions. • Approve the VP 7 (electronic voucher) transaction document before the designated date. • Changes to Default Account Codes, and/or identified employees for approval authorizations (reviewer and/or final approver should be provided to the procard Office at time of change.

HISTORICALLY UNDERUTILIZED BUSINESS (HUB)

<p>15. My area/department is committed to the University's goal of doing business with Historically Underutilized Businesses (HUBs) and I ensure HUBs are considered in the selection of vendors and contractors paid from my Accounts.</p>	<p>UTSA HUB Program Web site UTSA's Purchasing Office Web Site HOP 9.26 - Historically Underutilized Business Program</p>	<ul style="list-style-type: none"> • Gain a working knowledge of UTSA's HUB Mission Statement. • Take steps to ensure HUB vendors are utilized whenever possible on purchases under \$5,000. • When applicable, utilize HUB information provided by the HUB Office or the Purchasing Office to make purchasing decisions. • HUB vendors can be found on the State of Texas Centralized Master Bidders List (CMBL) maintained by the Texas Comptroller's Office
---	---	--

<http://www.window.state.tx.us/procurement/prog/cmb/> or the UTSA HUB Office Web site at <http://utsa.edu/hub/>.

BUSINESS SERVICES CONTRACTS AND LEASES

<p>16. I am aware and all employees paid from my Accounts (as applicable) have been informed that we do not have the authority to bind the University to a contract.</p>	<p>Regent's Rules Series No: 10501</p> <p>HOP 4.15 - Power to Bind the UT System</p> <p>UT System Policies: UTS145, Processing of Contracts</p> <p>UTS126, Processing of Space Lease Agreements</p> <p>UTS128, Consulting Contracts Policy and Procedures</p> <p>Procurement Contracts Office Web site</p>	<ul style="list-style-type: none"> • Ensure contracts comply with applicable UTSA and UT System contracting policies and procedures, including the Board of Regents' Rules and Regulations related to contract delegation. • The Board of Regents' Rules and Regulations require that all contracts be approved by the President or his/her official, authorized delegate (ref. Series 10501, §§ 5 & 6). Only an individual with a written delegation of authority from the President may execute and deliver contracts on behalf of the University. A University contract without an authorized signature may be invalid and unenforceable. <p>Resources and offices for processing contracts are:</p> <ol style="list-style-type: none"> 1. The Office of the Associate Vice President for Administration 2. Purchasing & Distribution Services Department
--	--	--

CAPITAL ASSETS MANAGEMENT

<p>17. An annual inventory of University property is conducted on items listed under my unit code(s).</p>	<p>UTSA Inventory Web site</p> <p>UTSA Handbook of Operating Procedures – 8.02 – Property Accounting Responsibilities</p> <p>Financial Management Operational Guidelines – Section 14 – Property and Equipment Management and Control</p>	<ul style="list-style-type: none"> • The Inventory Contact Person (ICP) is a staff/faculty member responsible for daily oversight of the department's inventory. • Ensure the department designates a primary and/or alternate ICP and submit an ICP Appointment Form at the beginning of each fiscal year to the Inventory Department. • The Inventory Department will determine what type of training is needed (initial or refresher) and contact the ICP to schedule the training needed to conduct the department's annual inventory. • Contact the DEFINE Administrators and ensure the ICP has access to inventory records for each Unit Code that ICP is responsible for updating in DEFINE. • Ensure your department's annual inventory is conducted and review the annual inventory documentation before completing the required annual certification. • Although not required by policy, it is a good management practice to structure duties so the individual maintaining inventory records does not also perform the annual physical inventory (if staffing permits). In addition, it is also recommended a second person accompany the person performing the annual inventory.
<p>18. Proper inventory forms are prepared and maintained for all asset items under my unit code(s). In addition, during the annual inventory process, employees with inventory items listed under my unit code(s) are required to sign the Inventory Custody Form, providing</p>	<p>UTSA Inventory Web site</p> <p>UTSA Handbook of Operating Procedures – 8.02 – Property Accounting Responsibilities</p>	<ul style="list-style-type: none"> • Designate an employee(s) to oversee the inventory process. • UTSA Inventory Forms are available in all categories related to managing UTSA assets.

<p>their Banner ID, for the inventory items assigned to them. DEFINE's inventory records are updated to reflect the appropriate custodial employee's Banner ID.</p>	<p>Financial Management Operational Guidelines – Section 14 – Property and Equipment Management and Control</p>	
<p>19. Equipment vulnerable to theft in my area/department is adequately safeguarded in locked cabinets and locked rooms.</p>	<p>UTSA Inventory Web site</p> <p>Controlled Property Class Codes</p> <p>State Property Accounting – Fiscal Policies & Procedures: SPA Process User's Guide, Appendix A</p>	<ul style="list-style-type: none"> • Ensure items such as cameras, laptops, projectors etc. are in locked rooms or cabinets when not in use and limit the number of individuals who have keys/access.
<p>20. In the event that equipment is stolen or recovered, I and/or an employee in my area will notify the University Police Department and the Inventory Manager as required by University policy. In addition, I am aware and all employees paid from my Accounts (as applicable) have been informed that they may be held personally liable for lost/stolen equipment if:</p> <ul style="list-style-type: none"> • Reasonable care was not exercised in the safekeeping, maintenance and service of the equipment; or • The loss occurred as a result of an intentional wrongful or negligent act. 	<p>UTSA Inventory Web site</p> <p>Financial Management Operational Guidelines – Section 14 – Property and Equipment Management and Control</p>	<ul style="list-style-type: none"> • Ensure employees are familiar with rules regarding accountability for university property. • Contact the University Police at 458-4242 and an officer will be assigned to investigate. • After contacting University Police, contact the Inventory Department and complete and submit an official Stolen/Recovered Property Report with a copy of the police report. • If stolen off-campus and not investigated by University Police, the theft must also be reported to University Police. University Police will create a Dispatch Report. A copy of this Dispatch Report and the police report from the investigating police department must be submitted with the Stolen/Recovered Property Report to the Inventory Department.
<p>21. All separating employees paid from my Accounts have returned all equipment assigned to them and have been cleared by my area's Inventory Contact Person before leaving the University.</p>	<p>UTSA Inventory Web site</p> <p>Employee Separation Processing Form</p>	<ul style="list-style-type: none"> • Ensure separating employees are cleared by the designated ICP. • Must receive inventory confirmation from the Inventory Department that the separating individual is cleared of any obligations.
<p>22. All equipment listed under my unit code(s) that is taken off-campus is returned to my area when no longer used for University business, and I ensure that my area maintains complete records for all University-owned equipment listed under my unit code(s) that is not on University premises.</p>	<p>UTSA Inventory Web site</p> <p>Removal of Equipment Form</p> <p>Financial Management Operational Guidelines – Section 14 – Property and Equipment Management and Control</p>	<ul style="list-style-type: none"> • A Removal of Equipment Form must be completed before any university property can be removed from university premises. This form requires the signatures of the authorized department official and the appropriate dean or vice president. Verify that laptops/notebooks being removed from campus have been encrypted or has been formally approved for waiver by OIT.
GIFTS		
<p>23. All gifts to the University shall be deposited within 24 hours of receipt with the gift services unit of the Office of University Advancement (OUA). All campus units are to deliver</p>	<p>Regent's Rules Series No: 60101</p>	<ul style="list-style-type: none"> • Review information on UTSA's Office of University Advancement Web site. • Managers should have a working knowledge of gift policies in the HOP and Regents' Rules (see web links provided)

<p>cash/checks/credit card gifts and other cash equivalents along with a completed Gift Processing Form and all related documentation from the donor to Office of University Advancement. When the gift is deposited, the donors will receive a tax receipt and an acknowledgment letter thanking them for his/her gift from our donor relations/development officer. In-Kind gifts are processed using the Gift In-kind Acceptance form which is processed through the respective Dean's office and delivered to Office of University Advancement for completion. Receipts and acknowledgement letters are issued in conjunction with the formal acceptance of in-kind gifts.</p> <p>Note: For UTSA purposes, "gifts" are described as "a contribution of cash or gift-in-kind in which the donor voluntarily gives us all control of the asset to the University for its benefit."</p>	<p>UTSA Handbook of Operating Procedures – 9.23 - Procedures Governing Private Gift Solicitation</p>	<ul style="list-style-type: none"> • Ensure designated employees know where to find and how to fill out the Gift Processing Form and the Gift In-Kind Acceptance Form. • Ensure employees know contact information for the unit/college Development Officer (if applicable) or the UTSA Development Advancement Services Office. • Procedures for receiving Gift checks should be followed in the same manner as any cash and/or check transaction, e.g. segregation of duties, log, etc. • Use the Gift Transmittal List Form to record gifts delivered to the VPUA office; this is the delivery receipt vehicle.
<p>24. There is a process in my area/department to ensure each donor receives a tax receipt. Development and Advancement Services then issue an acknowledgment letter thanking the donor.</p>		<ul style="list-style-type: none"> • The Manager of Gift Services and the Director of Endowment Compliance and gift Services work together to manage gift accounts and reconcile data with UTSA fiscal services. • There are written procedures on managing gift accounts. • Files are kept current, organized and easily identifiable in electronic format. Copies of gift documentation are scanned and confidential information is redacted. Access to this information is restricted and not readily accessible to non-departmental staff. • Files contain copies of the Gift Processing Form, any correspondence from the donor, check, and department chair/director's acknowledgment letter. (All original documentation is forwarded to the Development and Advancement Services Office.) All credit card or bank account numbers are removed or hidden on retained paperwork.
<p>25. There is a process in my area/department to keep track of all gift accounts for which we are responsible and ensure that current files are maintained.</p>		<ul style="list-style-type: none"> • See above #24.
<p>26. All gift accounts for which I am responsible are maintained with current information and all expenditures from these accounts are in accordance with donor's wishes. Accounts managed by other units are periodically monitored for compliant expenditures.</p>	<p>Regent's Rules Series No: 60202</p>	<ul style="list-style-type: none"> • Designate an employee to manage gift accounts. • Document policies/procedures for expenditures including donor's intentions for each gift account. • Ensure employees know policies and procedures regarding appropriate expenditures. • Prior to approving expenditures from gift accounts, ensure the

		expenditure is in compliance with the donor's intentions.
HUMAN RESOURCES		
<p>27. I complete and document annual performance evaluations for all employees reporting directly to me and I have a process in place to ensure annual performance evaluations are performed for all other employees who are paid from my Accounts.</p>	<p>UTSA Handbook of Operating Procedures - Annual Non-Faculty Performance Evaluation</p> <p>UTSA Handbook of Operating Procedures – Annual Faculty Performance Appraisal</p> <p>http://www.utsa.edu/hr/forms.cfm#7</p>	<ul style="list-style-type: none"> • Every supervisor is expected to conduct an annual performance evaluation for all regular Classified and Administrative and Professional employees that report to them. Standard Evaluation Forms are available on the Human Resources Web site. • Evaluations should be completed no later than the first work day in March of each year covering the period Feb 1st of the previous year through Jan 31st of the current year. • Place the original evaluation form in the employee's departmental personnel file and provide a copy to the employee and a copy to the Department of Human Resources. • Ensure probationary employees are evaluated during the first six months of employment. An evaluation should be conducted on the 30th, 90th, and 160th day of employment. Results of these evaluations should be the basis for retention or release of the employee. Probationary Evaluation Forms are available on the Human Resources Web site. • Develop performance standards for all positions (you may consult with your employees when developing standards for the position). • Communicate the standards for the position to the employee upon hiring and at the onset of the evaluation period. • In evaluating an employee, consider the employee's performance in the position in relation to the standards previously set by the supervisor.
<p>28. My area has a process in place to record and track activity for hourly employees paid from my Accounts, including ensuring overtime and other non-work hours are appropriate and approved in advance by a supervisor.</p>	<p>Payroll Office Web site</p> <p>Payroll Forms</p> <p>Payroll Calendar</p>	<ul style="list-style-type: none"> • Time sheets/cards should be used to record hours worked for hourly employees and are available on the Payroll Web site: hourly employee time card. • Time sheets/cards should be signed and dated by the employee and supervisor and kept on file in the department. • Hourly employees are generally paid on a semi-monthly basis. Ensure that the electronic payroll voucher (OV1) is created and approved by the payroll deadline on the payroll calendar.
<p>29. There is a process in my area/department to ensure overtime and other non-standard work hours are appropriate and approved in advance by a supervisor.</p>	<p>UTSA Handbook of Operating Procedures - Overtime Payments</p>	<ul style="list-style-type: none"> • Whenever possible, notify employees in advance when business demands require they work non-standard or overtime hours. • Develop a departmental procedure for requests to work additional or nonstandard hours (explanation for supervisor, supervisor's approval, etc.) and keep copies of documentation.
<p>30. My area has a process to manage employee leave for employees paid from my Accounts that achieves the following:</p> <ul style="list-style-type: none"> • Employee workdays are monitored and leave balances are routinely reviewed by 		<ul style="list-style-type: none"> • Ensure the department keeps copies of appropriate documentation/records. • Encourage employees to review their individual reports for accuracy.

<p>someone in their management chain.</p> <ul style="list-style-type: none"> • Vacation, sick leave and compensatory time balances are reconciled and entered to DEFINE on a monthly basis. • Leave balances (vacation, sick and compensatory) are communicated to employees on a monthly basis. • Monthly Vacation & Sick Leave Report reflecting the prior month's leave activity is submitted to HR by the 15th of each month. 		
<p>31. All qualified job applicants are considered and HR guidelines for determining the best-qualified applicant are followed when hiring employees paid from my Accounts.</p>	<p>HR Recruitment Guidelines</p> <p>UTSA Handbook of Operating Procedures - Records and Information Management and Retention</p>	<ul style="list-style-type: none"> • A set of job related interview questions should be prepared in advance of the interviews. • Interview questions should be designed to permit a fair and objective evaluation of each applicant and consist of objective, job-related inquiries. • Each applicant should be asked the same questions; all responses should be recorded in writing. A list of acceptable questions can be found at: Sample Interview Questions. • To facilitate the hiring decision, a matrix should be used. • Use the applicant screening matrix to screen applicants for interviews: Applicant Screening Matrix. • Use the interview matrix to assist in selection of a “finalist” from the interview process: Interview Matrix • The matrix, questions and responses should be maintained by the department for a minimum of two years.
<p>EEO COMPLIANCE</p>		
<p>32. I am aware and all employees paid from my Accounts (as applicable) have been informed that sexual misconduct and sexual harassment in any form will not be tolerated, the offending employee may be subject to disciplinary action, and that all incidents are to be reported to Equal Opportunity Services immediately.</p>	<p>UTSA Handbook of Operating Procedures - Nondiscrimination and Sexual Harassment and Sexual Misconduct</p> <p>UTSA Handbook of Operating Procedures - Consensual Relationships</p> <p>Office of Equal Opportunity Services Web site</p>	<ul style="list-style-type: none"> • Recognize sexual harassment includes conduct that interferes with an individual’s work performance or creates an intimidating, hostile or offensive work environment. Sexual harassment may include telling sexually explicit jokes, making inappropriate comments, or sending e-mails to one another containing jokes of a sexual nature. • Offensive behavior and comments in the workplace can constitute a hostile work environment, even if other people deem such conduct harmless, insignificant or they take no offense to it. • A workplace can easily develop into a culture that tolerates inappropriate behavior and comments if it is not addressed. This creates the potential to: negatively impact employees and the work environment, fall below acceptable standards for professional conduct and create a sense of discomfort that results in behavior that violates university policy. • Set expectations, communicate them to your employees, and remind employees about the sexual harassment policy and procedures. • Ensure employees know where in the HOP they can find the policies on nondiscrimination and sexual harassment and sexual misconduct. • Ensure you comply with the sexual harassment policies and procedures

		<p>by not initiating inappropriate actions, participating in inappropriate discussions, or condoning such actions or discussions by choosing to remain silent.</p>
<p>33. I am aware and all employees paid from my Accounts (as applicable) have been informed that various forms of discrimination, including discrimination based upon any protected category, including sexual orientation, is prohibited by state and federal laws and/or by University policy, and that all incidents are to be reported to Equal Opportunity Services immediately.</p>	<p>UTSA Handbook of Operating Procedures - Nondiscrimination and Sexual Harassment and Sexual Misconduct</p> <p>UTSA Handbook of Operating Procedures - Consensual Relationships</p> <p>Office of Equal Opportunity Services Web site</p> <p>United States Equal Employment Opportunity Commission</p>	<ul style="list-style-type: none"> • Recognize your role and responsibilities as a manager in taking action to prevent discrimination, including: <ul style="list-style-type: none"> ○ Examining your own behavior and making sure you lead by example. ○ Identifying early signs of unprofessional behavior that may require preventive measures. ○ Identifying specific behaviors requiring proactive measures or immediate intervention. • UTSA prohibits discrimination in all areas of employment, including recruitment, hiring, training, assignments, promotion, discipline and termination. • Employment discrimination occurs if it is based on race, color, religion, sex, national origin, age, disability, veteran status, or sexual orientation. • Examples of employment discrimination include: <ul style="list-style-type: none"> ○ Treating one employee differently than another who is similarly situated. ○ Any employment practice no matter what the intent, if it has a disparate impact on members of a protected class, which includes women, minorities, individuals with disabilities, veterans, and persons over 40 years old.
<p>34. I am aware and have informed my area/department staff to refer individuals reporting incidents of sexual harassment and/or discrimination to contact the Office of Equal Opportunity Services (EOS) immediately.</p>	<p>UTSA Handbook of Operating Procedures - Nondiscrimination and Sexual Harassment and Sexual Misconduct</p> <p>UTSA Handbook of Operating Procedures - Consensual Relationships</p> <p>Office of Equal Opportunity Services Web site</p>	<ul style="list-style-type: none"> • The Office of Equal Opportunity Services (EOS) investigates complaints of discrimination and harassment for students, faculty, staff and visitors/guests of the university.
<p>35. I am aware and have informed my area/department staff that all complaints of sexual harassment and/or discrimination should be filed as soon as possible after the conduct giving rise to the complaint.</p>	<p>UTSA Handbook of Operating Procedures - Nondiscrimination and Sexual Harassment and Sexual Misconduct</p> <p>UTSA Handbook of Operating Procedures - Consensual Relationships</p> <p>Office of Equal Opportunity Services Web site</p>	<ul style="list-style-type: none"> • As a university official, report incidences and/or complaints to EOS immediately. • Review information on the EOS Web site and encourage employees to review the site and make note of the contact names and numbers. • Reports of incidents of discrimination and harassment beyond the 30-day deadline should still be reported to EOS in order to determine the possible recurrence of past conduct.

<p>36. I am aware and all employees paid from my Accounts (as applicable) have been informed that it is unlawful to retaliate against an employee who has reported an allegation of wrongdoing or is participating in an investigation pertaining to allegations of wrongdoing.</p>	<p>Whistleblower Policy</p>	<p>UTSA is committed to an environment which prohibits retaliation for engaging in protected activities such as reporting or filing an EOS complaint of discrimination or harassment</p> <ul style="list-style-type: none"> • Encourage employees to report allegations of discrimination and harassment. • Prohibit unlawful retaliation against employees for reporting and/or participation in an investigation pertaining to discrimination and harassment.
---	---	---

ENVIRONMENTAL HEALTH, SAFETY AND RISK MANAGEMENT		
<p>37. There is a process in my area/department to ensure departmental activities comply with applicable rules, regulations, and best practices relating to occupational health, safety and the environment to include:</p> <ul style="list-style-type: none"> • Purchase, use and disposal of hazardous chemicals, radioisotopes, and biological agents; • Purchase, use and disposal of certain equipment designed to emit, or that contains hazardous source material, to include class 3b and 4 lasers, scintillation counters, and x-ray producing machines. • Purchase, use and disposal of certain equipment to include biological safety cabinets (BSC's) and chemical fume hoods that are designed to contain potentially hazardous materials. • Proper preventative measures for maintaining equipment and facilities in a safe working order for all employees, students and visitors; and • Enrollment in the UTSA Occupational Health Program of employees who drive a commercial bus, or work with class 3b or 4 lasers, asbestos containing materials, research animals, or have routine exposure to bloodborne pathogens, high levels of noise, or other certain hazardous chemicals or biological agents that require respiratory protection / protective vaccinations; and Keeping my work area in compliance with NFPA 101 - Life Safety Code as mandated by the State Fire 	<p>Office of Environmental Health, Safety and Risk Management Web site</p> <p>UTSA Handbook of Operating Procedures - Occupational Safety and Health Policy</p> <p>UTSA Handbook of Operating Procedures - Procedures for Compliance with the Texas Hazard Communication Act</p> <p>UTSA Handbook of Operating Procedures - Hazardous Waste Management Program</p>	<ul style="list-style-type: none"> • Inform your staff that policies and safety manuals governing health and safety are referenced on the Web site for the Office of Environmental Health, Safety and Risk Management.

<p>Marshal's Office and UT System.</p>		
<p>38. There is a process in my area/department to ensure department staff attend applicable safety training courses mandated by the UTSA Environmental Health, Safety, and Risk Management Office (EHS&RM), State of Texas and federal regulations to include:</p> <ul style="list-style-type: none"> • Texas Hazard Communication Act, Radiation Control Program, Radioactive Material License and TX Blood Borne Pathogen Rule; and • Texas Commission on Environmental Quality (TCEQ) and Federal EPA/OSHA regulations governing hazardous waste operations. 	<p>Office of Environmental Health, Safety and Risk Management Web site</p> <p>Training and Development</p>	<ul style="list-style-type: none"> • Ensure employees attend the hazard communication safety training <u>prior</u> to working with hazardous chemicals or toxins. • Ensure employees attend radiation or laser safety training <u>prior</u> to working with radioactive materials or class 3b or 4 lasers. • Ensure employees who may be exposed to human blood, cells, tissues and body fluids attend initial bloodborne pathogens training, are offered the HBV Vaccine, <u>within 10 working days</u> of their assignment to work with these materials. Annual refresher training is also required for these employees. • Ensure employees working with biological agents or recombinant DNA in laboratories attend bio safety and laboratory safety training <u>prior</u> to working with these materials. • Ensure any employee, contractor, or visitor that requires access to a high containment select agent & toxin (BSL-3) facility for any reason, has received proper security clearance and entry/exit training as mandated by the UTSA Select Agent Program and the CDC. Contact the EHSRM Office @ 458-5250. • Ensure employees generating hazardous biological, chemical or radioactive material waste attend Hazardous Waste Generator's Safety Training <u>within 90 days</u> of being assigned to work with these materials. • Training is mandated by the following rules and regulations: TX Department of State Health Services (TDSHS) in the Texas Hazard Communication Act, TDSHS Radiation Control Program - Radioactive Material License for UTSA and TX Bloodborne Pathogen Rule; and federal CDC/USDA Select Agent Rules and TCEQ / EPA / OSHA regulations governing hazardous waste operations.
<p>39. I am aware and employees paid from my Accounts (as applicable) have been informed that it is important to be responsive to any safety, health or environmental concerns raised by faculty, staff or students and to report all employee accidents, injuries and exposures to hazardous agents to EHS&RM, regardless of whether they were formally reported by the employee. In addition, there is a process in my area to maintain contact with employees who have lost time due to injuries and encourage them to return to work within the scope of restrictions placed upon them by authorized treating physicians.</p>	<p>UTSA Handbook of Operating Procedures - Occupational Safety and Health Policy</p> <p>UTSA Handbook of Operating Procedures - Procedures for Compliance with the Texas Hazard Communication Act</p> <p>UTSA Handbook of Operating Procedures - Hazardous Waste Management Program</p> <p>Office of Environmental Health, Safety and Risk Management Web site</p>	<ul style="list-style-type: none"> • Contact Environmental Health, Safety, and Risk Management Office at 458-5250 if there are any concerns or questions. • Refer to the Office of Environmental Health, Safety and Risk Management Web site for specific contact persons, information and forms for reporting injuries or exposures, and the UTSA Return to Work Program. • Dial "911" on campus phone for emergencies. • Off campus and cellular phones dial 458-4911 to contact the UTSA Police Department in an emergency (non-emergency number is 458-4242). • The UTSA Police maintain emergency contact information for EHS&RM personnel to respond to accidents, fires, hazardous material spills and other emergencies as necessary

<p>40. There is a process in my department to ensure that specialized equipment deemed critical to departmental operations has been risk assessed and adequately insured.</p>	<p>Office of Environmental Health, Safety and Risk Management Web site</p>	<ul style="list-style-type: none"> • Most equipment falls under UTSA's general Comprehensive Property Protection Plan insurance coverage which has a \$250,000 deductible. All claims over \$25,000 must be reported to UT System Office of Risk Management. (UT-ORM) and should be routed through UTSA's Risk & Life Safety Manager • UT-ORM offers low deductible insurance coverage for equipment valued under \$250,000. Contact the UTSA Risk & Life Safety Manager at 458-4420 to assist with the equipment risk assessment and obtain insurance coverage.
UNIVERSITY POLICE		
<p>41. I am aware and employees paid from my Accounts (as applicable) have been informed that emergencies, crimes, illegal activity, suspicious packages and dangerous or potentially harmful events should be reported to the University Police Department immediately.</p>	<p>UTSA Administrative Memorandum No. 62: Injuries, Emergencies and Related Matters</p> <p>UTSA's Business Continuity and Emergency Management Office</p>	<ul style="list-style-type: none"> • Dial "911" on any campus phone to reach the University Police. • Ensure a list of essential phone numbers and contact persons is available and can be easily accessed by all employees. • All employees should know that University Police is located at PP 1.320. • Information regarding reporting crimes and hazards can be found on the University Police Web site. • Employees should be aware of and review UTSA Administrative Memorandum No. 62: Injuries, Emergencies and Related Matters
<p>42. I am aware and have informed my area/department staff to contact University Police if illegal activity is suspected.</p>	<p>University Police</p>	<ul style="list-style-type: none"> • Dial "911" on any campus phone to reach the University Police. • Ensure a list of essential phone numbers and contact persons is available and can be easily accessed by all employees. • Information regarding reporting crimes and hazards can be found on the University Police Web site. • All employees should know that University Police is located at PP 1.320.
KEY AND CARD ACCESS		
<p>43. I am aware and all employees paid from my Accounts (as applicable) have been informed that lost or stolen keys or access ID cards should be reported to be reported to the University of Texas at San Antonio Police Department (UTSAPD) and Access Services immediately.</p>	<p>UTSA Handbook of Operating Procedures - Keys to University Facilities</p>	<ul style="list-style-type: none"> • Managers should be aware of the policies regarding keys and access to university facilities. • Managers should ensure their employees know and adhere to university policy on keys and access to university facilities.
<p>44. Only the appropriate administrative head of an academic or administrative department is allowed to request keys being assigned to employees. There is a process in my area/department to ensure that keys or access ID cards for new employees are obtained by sending the employee's information to the Access Services Office.</p>	<p>UTSA's Access Control Information</p>	<ul style="list-style-type: none"> • All employees should know the Access Services Office is located at PP 1.402 and can be contacted at 458-6486. • The Access Request Authorization form is available on the Access Control section of the UTSAPD Web site.

EMERGENCY PREPAREDNESS		
45. I am aware and have informed my area/department staff of emergency evacuation procedures.	Comprehensive Emergency Management Plan	<ul style="list-style-type: none"> Managers should ensure their employees are familiar Comprehensive Emergency Management Plan. Ensure a list of essential phone numbers and contact persons is available and can be easily accessed by all employees. Know your building captains. Managers can obtain the name and contact number of the appropriate Floor Captain Safety Liaisons in their building at the Business Continuity and Emergency Management Web site.
46. I am aware and all employees paid from my Accounts (as applicable) have been informed of emergency evacuation procedures and that all employees are required to participate in all evacuation drills.	Community Emergency Response Guide (located near the entrance of every classroom and meeting room)	<ul style="list-style-type: none"> Communicate to employees that all evacuation drills should be taken seriously. Have a plan for helping employees who need additional assistance in an evacuation.
47. I know who my Floor Captain Safety Liaisons are and have informed my area/department staff they should refer to the Business Continuity and Emergency Management Web site for information regarding Floor Captain Safety Liaisons.	Comprehensive Emergency Management Plan Training: See the Safety Section of the Training & Development Class Schedule.	<ul style="list-style-type: none"> Know your Floor Captain Safety Liaisons. Managers can obtain the name and contact number of the appropriate Floor Captain Safety Liaisons in their building at the Business Continuity and Emergency Management Web site You are encouraged to participate in the Floor Captain Safety Liaison program.
48. I am aware and have informed my area/department staff that suspicious packages or devices should be immediately reported the University of Texas at San Antonio Police Department (UTSAPD).	FBI Advisory on Suspicious Packages UTSA's Business Continuity and Emergency Management Office	<ul style="list-style-type: none"> Review with employees the FBI Advisory on Suspicious Packages.
INFORMATION SECURITY		
49. All users of UTSA information resources in my area are aware of and comply with the requirements of the UTSA Password Standard , which include selecting a strong password, never disclosing, writing down or sharing account passwords and enabling a password-protected screen saver (or logging off) when computing devices are left unattended.	UTSA Handbook of Operating Procedures - Computer Security UTSA Handbook of Operating Procedures - Information Resources Use and Security Policy Internet Privacy UTSA's Password Standard	<ul style="list-style-type: none"> When assigning work or computers to your employees, ensure that each user has a separate computer account.
50. I am aware and have informed my	UTSA's Password Standard	<ul style="list-style-type: none"> When users leave their computers unattended, password protected

<p>area/department staff that all computers should have screensavers with password protection activated.</p>	<p>UTSA's Physical Access Standard</p>	<p>screensavers reduce the risk of access by an unauthorized user.</p> <ul style="list-style-type: none"> • Details on the procedure for activating a password-protected screensaver can be found at UTSA's OIT Computer Security Handbook.
<p>51. All users of UTSA information resources in my area are aware of and comply with the Software Licensing Standard requirements, including installing only properly licensed software on UTSA hardware, duplicating software only when legally permitted by the software license, and ensuring copyrighted materials (music, movies, intellectual property, etc.) are not downloaded, stored or shared via UTSA systems or networks unless expressly permitted by the copyright owner in accordance with Federal copyright laws.</p>	<p>UTSA Handbook of Operating Procedures - Reproduction of Copyright Materials</p> <p>UTSA's Software Licensing Standard</p> <p>UTSA's File Sharing Standard</p> <p>UTSA's Information Resources Acceptable Use Policy</p>	<ul style="list-style-type: none"> • State-owned computer equipment, including personal computers/servers and the UTSA network, may not be used to download or share copyrighted files. • In some cases, companies may permit the purchaser of a CD/DVD to make a single backup copy or may allow transferring of music files to a portable device. • If software is to be used in your office, check with the Office of Information Technology (OIT) or the Purchasing Department to ascertain the licensing status, before purchasing or duplicating the software. • Managers should ensure that their departments are in compliance with licensing rules for the various types of software used in their departments. • General Rules for Copyright
<p>52. I am aware and have informed my area/department staff to report information security incidents to the Office of Information Technology Security Team.</p>	<p>UTSA Handbook of Operating Procedures – Computer Security</p> <p>UTSA Incident Management Standard</p>	<ul style="list-style-type: none"> • An incident is the use of a computer to violate statutes or regulations; such misuse frequently results in disciplinary action. Be familiar with the Information Security policies and be sure that any irregular use of computing is reported. • The OIT Security team can be reached at these numbers: 458-5899, 458-7216 and 458-7218. If there is no answer, you may call 458-4555 and the staff will locate a member of the team. • UTSA's OIT Security Team will help you become familiar with the standards and practices that will help maintain security.
<p>53. I am aware and have informed my area/department staff to follow UTSA procedures, including calling OIT Support Services, when installing new computers or hooking up servers.</p>	<p>UTSA Network Access Standard</p> <p>UTSA Change Management Standard</p>	<ul style="list-style-type: none"> • Always check IT procedures before connecting to the network or installing new hardware. Follow the standard, check with the OIT Support Services and contact the OIT Security Team if you have specific questions. • In order to protect the integrity of the university's network, devices which have been connected without prior approval may be removed or otherwise be prevented from connecting to the network.
<p>54. All data stored in my area (paper-based and electronic, including email) has been evaluated to ensure it has a legitimate business purpose and is retained in accordance with policy requirements. It is critical that records be destroyed when the retention requirement has been met.</p>	<p>UTSA Handbook of Operating Procedures - Records and Information Management and Retention</p> <p>UTSA Data Classification Standard</p>	<ul style="list-style-type: none"> • Ensure information is removed or destroyed in accordance with the Retention Schedule.

	UTSA's Key Roles and Responsibilities	
<p>55. A review of all computers and/or servers in my area has been performed to determine whether sensitive or restricted data (Category I data per the Data Classification Standard) is being stored electronically and the data is physically and technically safeguarded to allow access only to those employees who need the information to perform their job responsibilities.</p> <p>Note: Category I data includes: Social Security numbers, health-related research data (e.g., human subjects), official transcripts, protected student data, credit card numbers, personnel information, financial data, etc.</p>	UTSA Data Classification Standard UTS 165 UTSA Handbook of Operating Procedures - Code of Ethics Secure Passwords	<ul style="list-style-type: none"> • Do not share passwords. • Lock up confidential information and restrict access. • Identify those within your office or department who might use confidential information and be sure they have been trained in the rules regarding privacy. • Be sure that backup tapes and computers with confidential information are not available to those who are not approved to handle such records. • Do not transmit personally identifiable information via e-mail or through other electronic means. • Annette Evans, Information Security Officer, 458-5899
<p>56. All laptops in my area/department containing sensitive or restricted data have been encrypted with Endpoint Encryption (formerly known as SafeBoot) or similar encryption software.</p>	UT System Security Practice Bulletin #1 UTSA Handbook of Operating Procedures – Confidentiality of SSN's UTSA's Data Classification Standard UTSA's Data Encryption Page	<ul style="list-style-type: none"> • Review the need for the sensitive data to be stored on a portable device. Is there another way to store the information? • In the event that you must store confidential data on your device, you are required to encrypt it using one of the recommended techniques listed on the Data Encryption Page.
<p>57. I have determined the frequency and extent to which backups will be performed of departmental data to match the information's importance and risk of loss in order to ensure business continuity.</p>	UTSA Handbook of Operating Procedures - Information Resources Use and Security Policy UTSA's Backup and Data Recovery Standard	<ul style="list-style-type: none"> • Create a backup and recovery plan that allows for business continuity in the event of data loss or no availability. • Offsite backup options should meet or exceed the UTSA standards as well as any applicable state laws. • Testing should be performed to ensure proper recovery will occur in the event of an outage. • The plan should be reviewed and updated yearly.