Internal Controls Manual

Office of Internal Audit and Management Advisory Services

Office of Enterprise Risk Management

Publication Date: February 16, 2012
Last Review/Revision Date: January 12, 2018

Introduction

Thank you for your interest in the East Carolina University *Internal Controls Manual*. This document is intended to serve as one of the tools that managers and employees can reference when developing business processes and carrying out their responsibilities for the University and our constituents. The University's mission of service requires a wide variety of tasks and assignments, completed by employees in numerous physical locations and with many diverse skills sets and backgrounds. Each of us has some level of University resources available to us as we complete our day-to-day tasks and projects. "Internal Controls" are the mechanism that allows us to minimize risk and protect the University's resources to ensure that they are used for legitimate purposes.

The concepts in this manual are offered as a starting point for your consideration. If you encounter unique situations, please call on us. We are ready to serve you.

*For issues related to risk identification, measurement and management, call the **Office of Enterprise Risk Management at 737-2803**.*
http://www.ecu.edu/erm/

*For issues related to internal controls and protection of University resources, call the **Office of Internal Audit and Management Advisory Services at 328-9025**.*
http://www.ecu.edu/audit/

Table of Contents

Introduction to Risk Management

One might ask why the concept of risk management would be included in an internal control manual. The reason is that risk management and internal control are interrelated. Usually when a risk is identified and depending on the risk treatment, management may identify a control(s) that will mitigate the risk; keeping in mind the control(s) should be cost effective and reasonable.

All activities of the University involve risk. There is no uniform risk management framework but the management of risk usually involves: (1) identifying the risk, (2) assessing the impact of the risk and the probability of occurrence, and (3) determining the risk treatment and risk owner.

Identifying the risk: process of recognizing and describing the risk. For example, an identifiable and recognized risk is the "inappropriate safeguarding of cash".

Assessing the impact: process of assessing the potential severity of impact (generally a negative impact, such as damage or loss) and the probability of occurrence. For example, without the proper internal controls cash could be stolen, which would result in a loss to the University and the probability of occurrence could be high.

Determining the risk treatment: process of deciding to avoid the risk, mitigate the risk, or doing nothing about the risk. In the example above, the process of avoiding the risk would result in not accepting cash, which is probably not an acceptable alternative as it could affect customer service. Doing nothing would not be acceptable either because of the high risk of loss. So probably the best treatment would be to implement the proper internal controls to ensure that cash is properly safeguarded.

Determining the risk owner: this is the person or entity that has the accountability or the authority to manage the risk. Normally, this is the person that has the overall responsibility of determining the risk treatment. In the example above, this could possibly be the Vice Chancellor for Administration and Finance.

The Office of Enterprise Risk Management (OERM) was formally established at East Carolina University in 2008. The mission of OERM is to, "Provide leadership and management experience to better identify and manage the university's strategic, financial, operational, regulatory compliance, and reputational risks holistically as an enterprise." For specific tools to help with assessing risks in your area, please contact the Chief Risk Officer at 252-737-2803.

Internal Control Concepts

Importance of Internal Controls

Think of internal control as a map that helps us get to our destination. Obviously, just because we have a map there is no guarantee that we will get there, but it does provide reasonable assurance. Internal controls enable the University to:

- Achieve goals;
- Carry out management directives;
- Reduce unpleasant surprises;
- Enhance the reliability of information;
- Promote effectiveness and efficiency of operations;
- Safeguard assets; and
- Comply with rules and regulations.

As servants of public trust, the East Carolina University community has a significant responsibility to utilize its resources in the most effective and efficient manner possible while remaining in compliance with laws and regulations. A strong system of internal controls is critical to properly manage University resources within all related business processes.

Objectives

The objectives of this reference manual are the following:

- ✓ To ensure understanding of management's responsibility to make certain that internal controls are established, properly documented, maintained, and followed by everyone from senior management down to the departmental level;
- ✓ To ensure understanding by all ECU employees of their responsibility for compliance with internal controls; and
- ✓ To provide guidance for managers and staff about the components of internal control, and provide tools to establish, properly document, maintain, and follow the University's system of internal controls.

Scope

Understanding internal controls applies to all University departments and operations. The examples of internal control activities in this manual should not be interpreted as an all-inclusive guide of all control activities appropriate for each department. With time, control processes can be expected to change to reflect changes in the operating environment.

How much control to employ is a business decision. When a weakness is identified in a control, management must choose among the following alternatives:

- Additional supervision and monitoring;
- Additional or compensating controls; and/or
- Accept the risk(s) associated with the identified control weakness(es).

This manual is not a substitute for existing policies and procedures. The guidance provided in this manual should be used in conjunction with existing policies and procedures.

Organizational Roles

Every employee of the University has a role in the system of internal control. Internal control is people-dependent. It is developed by people; it guides people; it provides people with a means of accountability; and people carry it out. Individual roles in the system of internal control vary greatly throughout any organization. Typically, an individual's position in the organization determines the extent of that person's involvement in internal control.

While everyone at the University has a responsibility for ensuring the system of internal control is effective, the greatest amount of responsibility rests with management. Management must ensure that the individuals performing the work have the skills and capacity for their position. Management must also provide employees with appropriate supervision, monitoring, and training so that the University can carry out its mission.

Internal Control

Internal control is a *process.* It is a means to an end, not an end itself. The goals of effective internal control include reliable financial reporting, effective and efficient operations, compliance with laws and regulations, and protection of the organization's resources. Internal control is affected by *people*. It is not simply policy manuals and forms, but people's actions across the organization.

Internal control enables ECU to stay on track toward fulfilling its objectives and achieving its mission. It also helps us to avoid surprises along the way and the negative public relations that can accompany a control breakdown. Internal control facilitates effective and efficient operations, reduces the risk from asset loss, and enables us to ensure compliance with laws and regulations. Internal control also facilitates reliable financial reporting by ensuring that all transactions are recorded and that all recorded transactions are factual, properly valued, recorded in a timely manner, properly classified, and accurately summarized and posted.

Some typical internal control concepts include, but are not limited to the following:

- Segregation of duties between employees;
- Safeguards over cash or other assets, such as locked safes or cabinets and key or badge access;
- Records of transactions;
- Review and approval of transactions by someone who does not prepare or process the same transactions;
- Adequate supervision over employees, control processes, work functions, or other activities; and
- Validation of transactions for accuracy and completeness by someone independent of preparing or processing the transactions.

The two types of internal controls are preventive controls and detective controls.

Preventive controls are intended to prevent or deter unwanted acts. They are considered proactive controls, intended to prevent loss, errors, or omissions. Examples of preventive controls are the following:

- Segregation of duties;
- Proper authorizations;
- Adequate documentation; and
- Physical security over assets.

Detective controls are intended to detect unwanted acts that have already occurred. These controls provide evidence after-the-fact of a loss or error, but do not prevent an occurrence. Detective controls play a critical part in providing evidence that preventive controls are working as intended and preventing losses from occurring. Examples of detective controls are the following:

- Supervisory review;
- Reports that identify the occurrence of specific transactions or events;
- Routine spot-checking;
- Variance analysis;
- Physical inventories;
- Control self-assessment; and
- Audits.

Control Conscious Environment

A control conscious environment is a critical element of internal control. It is an environment that supports ethical values and business practices. A control conscious environment conveys an attitude of honesty and accountability at all levels. It is a preventive control. Management is responsible for "setting the tone at the top" for their areas and encouraging the highest level of integrity and ethical behavior, as well as exhibiting leadership behavior that promotes internal control and accountability.

The list below includes suggestions for enhancement of a department's control environment. The list should not be considered all-inclusive, and each individual item may not be applicable to every department or unit at ECU. However, this should provide helpful guidance for promoting a more effective control environment.

- Ensure that University Policies, Regulations, and Rules (PRRs) are available to departmental personnel, in hard copy or via internet access.
- Ensure that all University departments and units have standard operating procedures that address critical activities, processes, and any issues which are unique to the department/unit.
- Ensure that employees understand University PRRs and standard operating procedures that apply to the duties and responsibilities for their position.

- Discuss ethical issues with employees. Ensure that employees are aware that ethics guidance is available. Furthermore, ensure that guidance is provided to those employees who need it.
- Ensure that employees are aware of their obligation to report questionable or unethical activities through their chain of command or to other University offices such as the Office of Internal Audit.
- Ensure that employees comply with the University's Conflict of Interest regulation and disclose potential conflicts of interest (such as employee or immediate family members' ownership interest in entities doing business or proposing to do business with the University).
- Ensure that job descriptions have been created, include responsibility for internal control within the job description, and ensure that the level of competence required for the job is adequately explained within the educational, skills, and experience requirements for the position.
- Ensure that the departments and units have an adequate employee training program.
- Ensure that employees receive timely performance evaluations.
- Ensure that employees are subject to an appropriate disciplinary process when not in compliance with policies, procedures, performance, or behavioral standards.

Key Control Activities

Key controls are those significant controls within our business processes, which if operating correctly will both ensure and give assurance that the University is achieving its key business objectives. Based on the specific process that management is attempting to control, many different controls and combinations of controls can be used. Key controls such as those listed below are put in place to meet management's business objectives.

- Authorization – Transactions are appropriately authorized by management;
- Accuracy – Transactions are properly calculated;
- Valuation – Appropriate measurement and recognition principles are applied;
- Completeness – All valid transactions are recorded;
- Classification – Transactions are properly classified;
- Existence – Recorded transactions occurred and were recorded only once;
- Timeliness – Transactions are recorded in the correct period;
- Safeguard assets – Assets are secured from theft, damage, and unauthorized access or usage; and
- Segregation of duties – Appropriate segregation between the authorization of transactions, the recording of transactions, and the maintenance of assets. (No single individual should control a transaction or process from start to finish without the participation or oversight of other parties.)

The following pages outline some of the most common, and most important, internal control activities.

Segregation of Duties

Segregation of duties is a preventive control that aids in the timely detection of errors and irregularities in the normal course of business by providing adequate checks and balances. Functions are separated so that no one person has control over all parts of a transaction. Roles and responsibilities must be clearly defined to ensure that no one person has complete control over more than one key processing function, such as authorizing, approving, certifying, disbursing, receiving, or reconciling.

The following functions should be separated among employees:

- Custody of assets;
- Record keeping;
- Authorization; and
- Reconciliation.

Ideally, no individual employee should handle more than one of the above-noted functions in a process. For example, the same person should not maintain custody of cash AND record the deposits. The same person should not record the deposits AND perform the reconciliations. A simple way of looking at segregation of duties is to have at least "two sets of eyes" look at a transaction.

Examples of segregation of duties among employees include:

- The person who requisitions purchases should not approve purchases;
- The person who approves purchases should not reconcile monthly financial reports;
- The person who maintains accounting records and reconciles financial reports should not have custody of checks;
- The person who opens mail and prepares the list of checks received, or receives payments in person, should not make the deposit; and
- The person who opens the mail and prepares the list of checks received, or receives payments in person, should not maintain accounts receivable records.
- A computer programmer who makes programming changes should not have access to publish the changes in the "production" environment.

Maintaining segregation of duties is especially challenging for departments and units with small numbers of employees. To compensate for this problem, some of the following steps should be considered:

- Create internal policies and procedures to specifically address separation of duties;
- Place greater emphasis on monitoring;
- Rotate responsibilities periodically, and require that when one person is on vacation, another person performs his/her duties (rather than letting them "pile up" to be completed upon the employee's return);
- Use transaction and activity reports (from ODS, ePrint, ecuBIC, etc.) to analyze activities; and
- Require restrictive endorsement of checks received immediately.

Reconciliations

Reconciliations are detective controls performed to verify that financial reports are accurate, complete, and timely, and to ensure that appropriate actions associated with a transaction or event have been taken. Financial reports containing revenue and expenditure account balances are relied upon to make financial and administrative decisions. Without timely reconciliations, there may be an increase in the risk of fraud, theft, or compliance violations.

Departmental account reconciliation is a comparison of a department's monthly financial reports to supporting documentation which is retained in the department. This control activity helps to ensure the accuracy and inclusion of all transactions that have been charged to the department's accounts.

Reconciliations should be performed to:

- Ensure that the expenditures that have been charged to the department's accounts were properly approved and charged to the correct account;
- Ensure that all revenues that have been earned and/or collected by the department have been credited and deposited to the correct account;
- Provide management with documented evidence that the general ledger account balances are valid, appropriate, approved, and adequate; and
- Discover accounting errors, omissions, and misclassifications in a timely fashion.

Listed below are suggestions to enhance the reconciliation process:

- Be sure to properly segregate duties - the person who performs departmental account reconciliations should not have access to the general ledger account or handle cash;
- Departmental account reconciliations should generally be performed monthly;
- The preparer and reviewer should both sign and date all account reconciliations;
- The reconciliation should have documented review and approval by someone other than the preparer;
- Reconciliations can either be paper based or electronic. Either format should include a header to identify reconciliation purpose and timeframe being covered; and
- All unusual reconciling items (differences noted during the reconciliation process) should be researched, resolved appropriately, and be documented thoroughly. Documentation should be retained for review by management or auditors.

Processes for reconciling departmental accounts include:

- Obtain monthly departmental financial reports from Banner, ODS, ePrint, ecuBIC or other resource;
- Compare beginning balances on current month's financial reports to ending balances on prior month's reports;
- Agree each expenditure and revenue transaction in the financial reports to supporting documentation, checking the mathematical accuracy of the reports;

- Note whether correcting entries from previous months' reconciliations have been posted to this month's financial reports. If not posted, it may be necessary to make a correcting entry; and
- Prepare a reconciliation report for management's review and approval.

Out-of-balance situations may occur due to the following scenarios:
- Natural timing differences;
- Misclassification (i.e. journal entry to the wrong account);
- Miscalculation;
- Errors where an entry was omitted or recorded multiple times; and
- Other unexplained reasons or a combination of reasons not yet identified.

Segregation of Duties and Reconciliation Example: In a department that collects payments from individuals, the person who receives the payments should not control the entire process. A separate individual should deposit the funds, and an individual who is not involved in the collection or deposit should compare the records of payments received with the reports of deposits made to the departmental accounts in Banner to verify that all funds were deposited.

Authorization, Approval, and Verification

Authorization is an important control activity that assures transactions are only permitted in accordance with management's directives. Authorization requires the signature or electronic approval of a transaction by someone who has approval authority. The approver should follow these guidelines:

- The approver should review any relevant supporting documentation and be satisfied that the transaction is appropriate, accurate and compliant with all applicable laws, policies, regulations, rules, and standard operating procedures.
- Any unusual items should be questioned to ensure that all necessary information is provided for justification prior to any approval. The failure of management to question what they sign and/or the "rubber stamping" of documents or transactions will circumvent the authorization controls.
- Under no circumstances should an approver tell someone else to sign the approver's name.
- In the case of electronic signatures, the approver's password should never be shared with another person.

Authorization in certain cases can be delegated; however, this delegation of authority should be on a limited "must have" basis with established parameters. Management should ensure that the conditions and terms of authorization are clearly defined, documented, and communicated.

Delegation of Authority for Contracts is documented at http://www.ecu.edu/PRR/01/10/01/, along with the ECU Delegations of Authority to Sign Contracts at http://www.ecu.edu/attorney/delegation.cfm.

Documentation

The term *documentation* means something that can furnish evidence or information regarding a decision, event, transaction, policy, or system. Documentation that is clear, complete, accurate and recorded timely adds to the efficiency and effectiveness of the University's goals. Documentation facilitates the performance of processes and procedures in a more efficient, consistent, and reliable manner since the procedures are standardized. Documentation serves as a method of training since it includes manuals and guides.

Documentation of transactions should enable management to trace each transaction from its inception through its completion. This means the entire life cycle of the transaction should be recorded, including: (1) its initiation and authorization, (2) its progress through all stages of processing, and (3) its final classification in summary records. For example, the documentation for the purchase of equipment would start with the authorized purchase request and continue with the purchase order, the vendor invoice and the final payment documentation.

***Documentation Example*:** In the previous scenario involving a department's collection of payments, the person who collects the payment should document the transaction using a pre-numbered receipt. The receipt should include the date, method of payment, amount of payment, and purpose. The receipt should be given to the payer, and a copy of the receipt should be retained in the department. The receipts should be used and issued in numerical order. (The departmental receipt copies would then be used by another person during the reconciliation process.)

Monitoring/Management Oversight

Monitoring is an ongoing evaluation of an organization's activities and transactions to determine whether the components of internal control within designated processes are working as intended. An internal control system can only be effective if the controls are functioning properly. Proper monitoring will help identify internal control deficiencies and determine whether the controls are effective in addressing any new risks.

Management's role is crucial in establishing an effective internal control system by ensuring the monitoring conducted is objective and is performed by personnel with sufficient knowledge to understand how the controls should operate and what would constitute a deficiency. Internal controls evolve over time and can become less efficient due to factors such as new personnel, varying levels of training and supervision, time and resource constraints, and changes in circumstances that may have occurred since the initial internal controls were designed.

Individual employees should routinely monitor and evaluate internal controls affecting their areas since they are involved in the daily activity of a process and are more attune to any changes/situations that may potentially influence the effectiveness of the internal controls. Management usually has time constraints that prevent analysis of every piece of information. For this reason, management should concentrate on their high-risk areas first and may use monitoring techniques such as spot checks of transactions, basic sampling techniques, or other methods that will provide a reasonable level of confidence that the controls are functioning as intended. An effective monitoring foundation is dependent on establishing an effective "tone at the top" within the department/unit and making effective internal controls a high priority.

Some examples of monitoring may include the following:

- Review reconciliations for accuracy and to confirm that all discrepancies are explained.
- Review of procurement card reconciliations for reasonableness.
- Surprise cash counts.
- Special account analysis for high risk accounts.
- Randomly pull a transaction's supporting documentation to ensure accuracy, reliability, appropriate approval, and reasonableness.

Access Controls (Logical Security)

Access to information systems, and to specific data and functions within the systems, should be granted only to individuals with a legitimate need for the access to perform their assigned functions. In general, an individual should have the lowest level of access that allows him/her to perform all of his/her duties.

Access to data and information systems must be protected by authentication and authorization controls. Improper access controls can severely impact the ability of the University to conduct educational and administrative business, and can lead to substantial fines in accordance with numerous federal and state privacy laws. An authentication control ensures the validity of user identification.

An example of an authentication control at ECU is the Pirate ID, a unique and verified user identification assigned to each employee and student. Generic identifiers such as "ECU001" should be avoided, since they do not allow the access to be attributed to a single identifiable individual. Authorization controls include passphrases subject to strength testing and forced expiration as outlined in the Security and Policies section of the ITCS homepage at http://www.ecu.edu/itcs/ .

Physical Security

Physical and environmental security encompasses multiple criteria.

- A secure perimeter should be established to prevent unauthorized access to critical or sensitive assets and/or data. The level of security should be based upon the criticality of the assets and/or data. Information system hardware and software that support key business processes should be in a secure area that not only protects the assets from unauthorized access but also protects against fire, flooding, and other natural or man-made disasters.
- Areas where access by unauthorized personnel is to be prevented should require identification badges be worn at all times. Visitors should be escorted within the facility. Unrecognized persons within the secure area should be challenged as to the reason for their presence and escorted out of the area using ECU Police if necessary.
- Issuance of keys and access badges should be strictly controlled and frequently reviewed (at least quarterly) to ensure access is granted only to those who need it. Access should be terminated immediately when employees transfer or leave the University.
- Employees should practice a "clear desk" policy to prevent unauthorized access to sensitive information and possible loss of or damage to sensitive information during non-working hours when offices cannot be locked. Papers and electronic media should be locked in drawers or cabinets when not in use, particularly during non-working hours. Sensitive documents, including electronic media, should also be locked when not in use or after business hours, preferably in a fire-resistant cabinet or safe.
- Incoming and outgoing mail drops, unattended printers, and unattended fax machines should be evaluated as to the need for restricted or secure access.
- Unattended computers and other electronic devices which allow access to University networks should have password controls and should be configured to automatically timeout during periods of inactivity, with password-protected login required to regain access.
    - Computers and other equipment removed from University property are governed by ECU Materials Management Policy at http://www.ecu.edu/cs-admin/purchasing/centralstores/Fixed.cfm#CP_JUMP_140971.
    - Removal of equipment from the University premises must be authorized and documented with an Equipment Tracking Form http://www.ecu.edu/cs-admin/purchasing/centralstores/upload/equipment_tracking.pdf. The form must be updated annually.
- Critical equipment, such as information systems hardware, should have adequate power supplies and uninterruptible auxiliary power. Equipment should be protected from power surges. Auxiliary power should be tested regularly to ensure operation when needed.
- Critical equipment should have adequate environmental support, including heat and air conditioning. The assets should be protected from exposure to water, smoke, chemicals, and dust.

- Fire suppression equipment should be installed to protect critical assets, including information systems. The fire suppression equipment should be capable of automatic and manual activation. The fire suppression equipment should be inspected and tested yearly. Portable fire extinguishers should be sufficient in number and location to cover the area where the critical assets are located. Personnel should be trained in the operation of the fire suppression equipment and the portable fire extinguishers. Fire and other emergency procedure drills should be conducted with all personnel.
- Data and power cables which service buildings should be underground or otherwise protected from disruption, interference, or interception of data.
- Assets, including information systems, should be maintained in accordance with manufacturer or vendor guidelines. Maintenance should be completed by authorized personnel. Records of maintenance should include periodic servicing, repairs, and performance faults or suspected faults.
- Desktop and laptop or other portable computers must have antivirus and antispyware software installed and active. Access to this equipment should be password-protected.
- Computers in use off campus should have access protection such as locks and password protection to guard against unauthorized access. Laptops and other portable electronic storage media should be encrypted whenever possible to prevent unauthorized access to the data stored on these media. Laptops and other portable devices should be included with “carry-on” luggage when travelling.
- All software should be properly registered to avoid licensing issues and enable identification of recovered equipment. Serial numbers of all computer hardware and other assets should be recorded.
- Computers sent to Surplus must be sent to ITCS for removal and destruction of the hard drive. Computers transferred to another primary user within ECU will have the hard drive reimaged by ITCS. See http://www.ecu.edu/prr/08/05/02 for details.
- Department heads are responsible for the security and inventory of all assets assigned to the department.
    - For items exceeding the threshold for classification as a “fixed asset”, Fixed Asset Inventory Verification Lists and Lost Inventory lists are available on ePrint in October of each year. Departments are notified by email when their reports are available for print and review. Guidelines for these reports are available on the Materials Management website. The reports must be completed, signed by the Department Head, and returned to the Fixed Assets Office, Central Stores and Receiving, 1150 S. Greene Street, Building 215C, by November 30th of each year.
    - Department heads are also responsible for the departmental assets that fall below the fixed assets accounting threshold. Inventory lists of valuable or “high risk” items such as computers, laptops, specialized equipment, cameras, etc. should be documented and reviewed at least annually.

Policies, Regulations, Rules (PRRs) and Standard Operating Procedures

A *policy, regulation or rule* establishes what should be done and is the basis for procedures. *Standard operating* p*rocedures* describe specifically how the policy, regulation, or rule is to be implemented. An organization must establish policies, regulations, rules, and standard operating procedures so that staff members know what must be done and so that compliance with the goals of the organization can be properly evaluated. If policies, regulations, rules and standard operating procedures are not clear, comprehensive, and effectively communicated, there is increased risk that decisions made and actions taken might not be in accordance with University PRRs and State and Federal laws. It is simply a good business practice to have available PRRs and standard operating procedures to guide actions of the department or unit. Written PRRs and standard operating procedures increase efficiency, reduce errors, and make training of new personnel easier and faster.

Developing PRRs and standard operating procedures can be a daunting task. The following steps may be helpful to the department.

- Don't reinvent the wheel. Be familiar with the existing University-wide Policies, Rules, and Regulations website. See Regulation 01.15.01 on Formatting, Adopting, and Publishing Polices, Regulations, and Rules.
- Assign one departmental employee with the responsibility and authority to lead a group in composing and updating standard operating procedures.

Timekeeping

Internal controls over the time and leave reporting processes are essential to ensure accurate and reliable reporting of time and leave balances. Failure to have effective controls may result in improper compensation due to inaccurate time reporting and leave balances. This discrepancy may be immaterial individually but material for the University as a whole.

Actual Timekeeping and Leave Policies can be viewed at the following links:

- East Carolina University's Human Resources has a SHRA/CSS Employee Manual that has descriptions and policies regarding time and leave reporting. See SHRA_CSS Employee Handbook.pdf http://www.ecu.edu/prr/06/20/02
- For Mass time entry instructions, see forms and instructions at the HR website: Mass_Time_Entry_Instructions.xls
- EPA leave policies, see http://www.ecu.edu/cs-admin/humanresources/CUSTOMCF/EPA_Administration/Management_Flexibility_Plan_and_Related_Policies/EPA_Employment_Policy.pdf
- Fair Labor Standards Act, see https://www.dol.gov/whd/flsa/

Timekeeping and Leave Best Practices:

- Communicate the internal leave reporting practices to unit employees at least annually.
- Departments should have documented procedures outlining their timekeeping process to ensure work time and leave reported are accurate, valid, and complete.
- Non-exempt employees (SHRA employees who are not exempt from the overtime provisions of the Fair Labor Standards Act) should record their time daily to ensure accuracy and timely reporting.
- All time entry submitted to payroll for payment should require supervisory approval.
- An employee should not serve as the supervisory approver of their own time reporting.
- An approver should have actual knowledge of the employee's work time and should be able to validate the accuracy of the time reported by the employee.
- One person per unit should be designated to update leave balances monthly and notify employees who fail to report their monthly balances.
- Mass Time Entry: The submitter or approver should ensure that the payment has not been submitted and paid via a web time entry form before processing a mass time entry form for payment.

Petty Cash Funds

The following guidelines are for those departments or units with an imprest cash (formerly called petty cash) fund.

- The custodian of the cash fund should be restricted from handling more than one fund and should not be involved in the cash receipts, collection, depositing, and reconciliation functions.
- The reimbursement vouchers should be approved by a responsible employee who does not have direct access to the cash.
- The cash fund should be replenished at least monthly.
- The cash fund must be properly authorized.
- Access to the cash fund should be restricted to the custodian and a back-up person.
- Cash requests should be signed by the person receiving the cash.
- Cash requests should be prepared in ink and required for each disbursement.
- Cash vouchers should be supported by an original receipt or invoice with the amounts and business purpose documented.
- Receipts and attachments should be properly cancelled to prevent their reuse.
- Maintain the original receipts or invoices in the cash fund box for reconciling.
- Cash funds should be verified by surprise counts. The cash funds are also subject to periodic unannounced counts by ECU Financial Services and ECU Office of Internal Audit.
- Cash fund disbursements should not exceed a fixed amount.
- Keep the cash fund in a locked, secure place to safeguard against theft.
- Cash should be disbursed only by the custodian (or a back-up person in the custodian’s absence).
- The cash fund should not be used for personal expenses; personal loans (IOUs), other unauthorized advances, or the cashing of personal checks.
- The custodian is responsible for regularly reconciling the cash fund.
- Investigate any unexplained cash shortage.

Cash Receipting

Cash is the most liquid of assets. This ready liquidity exposes the University to risk of loss unless cash is well controlled.

- Payments in person should be directed to the University Cashier, Division of Health Sciences Cashier, or ECU Physicians clinic cashiers as applicable.
- Change funds, or "tills" should be maintained at a minimum amount and employed only where necessary, such as a for cashier position.
- Payers should be presented a system-generated receipt or a receipt from a pre-numbered receipt book. Receipt books should be two-part; with one part given to the payer and one part retained affixed to the receipt book.
- Check numbers should be recorded on the receipt and the transaction number from the credit card electronic validator should be recorded on the receipt for credit card payments.
- Checks should be restrictively endorsed immediately upon receipt.
- Payments should be mailed to a central lockbox whenever possible. Payments inadvertently received by mail should be transported to a cashier in a secure method, preferably in a locked bank bag. Payments received by mail should be so indicated on the receipt.
- The receipts should agree with the payment log.
- Cash, checks, and credit card forms (when electronic validators not used) should be maintained in a locked and secure area, with restricted access.
- An employee with no cash handling duties should verify the amount of cash, checks, and credit card payments matches the amount on the receipts and log, where utilized.
- Departments receiving payments in error should forward such payments to the University or Health Sciences Cashier in a secure method, preferably in a locked bank bag, for research and disposition.
- A person independent of cash handling should prepare the deposit. Ideally, this will be the person who compares the payments received with the receipts and mail log.
- Deposits submitted to the University or Health Sciences Cashier should be transported in a locked bank bag.
- Departments should designate an employee to reconcile amounts collected with amounts deposited and posted to Banner. This person should not prepare the deposit.

Departmental management should perform the following on a periodic basis –

- Receipts should be reviewed for proper completion.
- Adjustments, including voids, should be reviewed for propriety and excessiveness, which could indicate insufficient training, skill, or irregularities.
- Surprise cash counts should be performed and documented by someone other than the fund custodian to ensure funds are intact.

See the segregation of duties matrices applicable to cash receipts at Appendix A and guidelines for separation of duties in offices with small staff levels in Appendix B.

Business Continuity Plan

ECU maintains business continuity/disaster recovery planning tips and information and sample business continuity plan templates on the Office of Environmental Health and Safety website. Departments are encouraged to use these templates and to consult with OEHS when developing and testing business continuity plans.

Backup and disaster recovery for electronic protected health information (EPHI) maintained by the University are outlined in Policy Security #0007 – Contingency Planning at http://www.ecu.edu/cs-dhs/hipaa/security/policies.cfm. The policies specifically address requirements to restore access to **exact** copies of EPHI. The policies further require annual employee training for disaster recovery, emergency operations for the continuance of critical processes that protect the security of information systems containing EPHI, annual or more frequent testing of disaster recovery and emergency operations, and annual criticality analysis of healthcare information systems and data.

A business continuity plan should outline how a department or functional area will complete its critical tasks during an emergency, or in the absence of a critical information system or other critical resource. The plan should include employee roles during an emergency. Computer hardware and other critical electronic equipment such as telephones and other two-way communications should have architecture and design, alternate (backup) hardware, and the processes for backup activities and system recovery, including expected recovery time, documented in the business continuity/disaster recovery plan.

The business continuity/disaster recovery plan should be tested to determine viability and to identify any weaknesses in the plan, which can be corrected and re-tested before an actual emergency arises. All personnel should be familiar with their roles in business continuity.

Appendix: Segregation of Duties for Primary Accounting Functions – Cash Receipts, Cash Disbursements, Payroll

(developed by the University System of Georgia)

Two-Person Office

Business Manager	Chief Financial Officer
Mail Checks	Approve and sign checks
Write checks	Sign employee contracts
Approve payroll	Distribute payroll
	Process vendor invoices
Record accounts receivable entries	Complete deposit slips
Receive cash	Reconcile petty cash
Disburse petty cash	Perform interbank transfers
Reconcile bank statements	Receive, open & review bank statements
Authorize purchase orders	Review bank reconciliations
Authorize check requests	
Authorize invoices for payment	
Record credits/debits in accounting records	
Record G/L entries	

Three-Person Office

Bookkeeper	Office Manager	Chief Financial Officer
	Mail checks	Sign checks
Record A/R entries	Disburse petty cash	Complete deposit slips
Reconcile petty cash	Approve invoices	Perform interbank transfers
Write checks	Authorize purchase orders	Sign employee contracts
Record general ledger entries	Approve payroll	Receive, open & review bank statements
Reconcile bank statements	Receive cash	Review bank reconciliations
Process vendor invoices	Distribute payroll	
Record debits/credits in accounting record	Authorize time sheets	

Four-Person Office

Bookkeeper	Clerk	Office Manager	Chief Financial Officer
Record A/R entries	Distribute payroll	Complete deposit slip	Sign checks
Reconcile petty cash	Receive cash	Approve invoices	Sign employee contracts
Write checks	Disburse petty cash	Approve payroll	Approve time sheets
Record G/L entries	Authorize POs	Process vendor invoices	Perform interbank transfers
Reconcile bank statements	Authorize check requests		Receive, open & review bank statements
Record debits/credits in accounting records	Mail checks		Review bank reconciliations