Authority **ORS 291.015**

Internal Control Framework

.101 The Committee of Sponsoring Organizations of the Treadway Commission (COSO) released a report in September 1992, that sets the national standards for **internal controls**. The report is titled Internal Control – Integrated Framework and consists of four volumes, including an executive summary. The COSO Report will be the basis for Oregon's internal control framework.

.102 Management of the State is responsible for establishing and maintaining internal control. Internal control is a process effected by management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

.103 According to the COSO model, internal control consists of five interrelated components, which are:

a. *Control environment* sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

Basic to the control environment are organizational structure, assignment of authority and responsibility, and human resources policy. More difficult to quantify are ethics, commitment to competence, and management operating style.

b. *Risk assessment* is the identification and analysis of risks relevant to achievement of objectives, forming a basis for determining how the risks should be managed.

Management's responsibility is to define compatible relevant objectives and the risks related to achieving those objectives. Management should have a basis for determining which risks are most critical. Management ensures mitigation of key operating risks.

c. *Control activities* are the policies and procedures that help ensure management directives are carried out.

Control activities reflect management's risk mitigation strategy in the form of directive, preventive, and detective controls. Focus is on achieving effectiveness and efficient resource usage as measured by the degree of achievement of control objectives.

Control activities help ensure necessary actions are taken to address risks relevant to achievement of objectives. Examples are physical controls and segregation of duties.

d. *Information and communication* are the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities. Information systems deal with both internally generated data and information about external events, activities, and conditions.

   Communication involves providing an understanding of individual roles and responsibilities pertaining to internal control. Management is obligated to communicate the standards of measurement for evaluating operations. In other words, sufficient relevant communication promotes cognizance of internal control objectives so employees understand how their individual actions interrelate and recognize how and for what they will be held accountable.

e. *Monitoring* is a process established by management that assesses the quality of internal control performance over time.

   Monitoring provides external oversight, either ongoing or in the form of independent checks of internal controls by management or other parties outside the process.

.104 Management should be committed to achieving strong controls through actions related to agency organization, personnel practices, communication, protection and uses of resources, and general leadership.

OREGON ACCOUNTING MANUAL		Number 10.10.00.PR
Oregon Department of Administrative Services State Controller's Division	**Procedure**	Effective Date July 1, 2001
Chapter	**Internal Control**	.1 OF .5
Part	**Management's Responsibilities**	
Section		Approval Signature on file at SCD

Authority **ORS 291.015**
ORS 291.038
ORS 293.590
ORS 293.595

Requirement to Maintain Adequate Internal Controls

.101 Each **agency head** is ultimately responsible for establishing, maintaining and improving the agency **internal controls**. The internal control of agencies must be adequate to provide reasonable, but not absolute, assurance that management's goals and objectives are being accomplished effectively and efficiently; assets are safeguarded; and transactions are accurate, properly recorded and executed in accordance with management's authorizations.

.102 All agencies are required to implement and maintain internal controls. Throughout the year, the **agency** will need to document periodic reviews, tests, and analysis of internal controls to assure proper operation. Agency management is responsible for the extent of efficiency and effectiveness of internal controls as well as any deficiencies therein.

.103 Each agency head may designate one senior agency manager as the internal control officer. This person's responsibility is for coordinating the overall agency-wide effort of annually (at a minimum) evaluating, improving and reporting on internal controls. The internal control officer provides assurance and documentation to the agency head that internal control review processes have been conducted. Each manager is responsible for review, evaluation and reporting for his/her particular part of internal control.

.104 Any material inadequacy or material weakness in an agency's internal control, including unresolved internal or external audit comments, should be identified. A plan and schedule for correcting any such inadequacy, including an estimated completion date, should be described in detail.

Components of Internal Control

.105 According to the Committee on Sponsoring Organizations of the Treadway Commission's (COSO) model, there are five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring. Effective internal controls promote accountability, facilitate achievement of agency goals and objectives, and ensure compliance with state and federal laws, rules, and regulations.

Control Environment

.106 The control environment encompasses the following factors:

a. *Integrity and ethical values.* Integrity and ethical behavior are the product of ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. Managers and employees are to maintain and demonstrate support of internal controls at all times. This support includes management's obligation to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. Also part of management responsibility is communication of values and behavioral standards to personnel through policy statements and codes of conduct and by behavioral example. Management's values should be corroborated by adequate supervision, training, and motivation of employees in the area of internal controls. To demonstrate support for good internal controls, management should emphasize the value of internal auditing and be responsive to information developed through internal and external audits.

b. *Commitment to competence.* Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Managers are required to comply with established personnel policies and practices for hiring, training, evaluating, promoting, and compensating employees, and to provide employees the resources necessary to perform their duties. Hiring and staffing decisions should include pertinent verification of education and experience and, once on the job, the individual should be given the necessary formal and on-the-job training.

   Counseling and performance appraisals are also important. Performance appraisals should be based on an assessment of many factors, one of which should be the implementation and maintenance of effective internal controls. Promotions driven by periodic performance appraisals demonstrate commitment to the advancement of qualified personnel to higher levels of responsibility.

c. *Management's philosophy and operating style.* Management's philosophy and operating style encompass a broad range of characteristics. Such characteristics may include management's attitudes and actions toward financial reporting (conservative or aggressive selection from available alternative accounting principles, and conscientiousness and conservatism with which accounting estimates are developed). Management's attitude should positively reinforce and personnel should support adherence to **Generally Accepted Accounting Principles (GAAP)** in the implementation of information processing and accounting functions.

   Managers should remain cognizant of the purpose of internal control with respect to accounting and reporting. The purpose of internal control is to help assure the assertions made by management in the accounting records and reports are materially correct with respect to existence, completeness (including proper period), rights and obligations, valuation, and presentation.

   In a government environment, evaluation of the cost of controls must be considered in light of legal and public policy framework. The controls in place should produce the largest net benefit, both quantitative and qualitative. Managers should periodically review for the optimum level of controls and eliminate unnecessary controls.

d. *Organizational structure.* An organizational structure provides the framework within which activities for achieving objectives are planned, executed, controlled, and monitored. Management should establish well designed organizational structures that incorporate the form and nature of the organizational units, including the data processing organization and related functions. For good internal control, management must require clear lines of authority and responsibility, appropriate reporting relationships, and appropriate separation of authority. The appropriateness of an organizational structure will depend, in part, on the size and nature of a unit's activities.

e. *Assignment of authority and responsibility.* This factor includes how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. Management should establish policies relating to appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, management should provide policies and direct communications so that all personnel understand the organization's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

   Proper segregation of responsibilities is a necessary condition to make control procedures effective. Management should ensure adequate separation of authorization for the execution of transactions, recording of transactions, custody of assets, and periodic reconciliation of existing assets to recorded amounts.

f. *Human resource policies and practices.* Human resource policies and practices relate to hiring, orientation, training, evaluating, counseling, promoting, compensating and remedial actions. To demonstrate commitment to competent and trustworthy people, management should establish and adhere to standards for hiring the most qualified individuals – with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior. Management is also required to implement training policies that communicate prospective roles and responsiblities. Training should be designed to illustrate expected levels of performance and behavior.

Risk Assessment

.107 Risk assessment is the identification, measurement, and management of risks relevant to the achievement of the organization's objectives. Risks include external and internal events or circumstances that may occur and adversely affect operations. Once risks are identified, management should consider their significance, the likelihood of their occurrence, and how to manage them. Management may initiate plans, programs, or actions to address specific risks or it may decide to accept a risk because of cost or other considerations. Risks can arise or change due to circumstances such as the following:

- *Changes in operating environment.* Changes in the regulatory or operating environment can result in changes in the competitive pressures which may alter risks.

- *New personnel.* New personnel may have a different focus on or understanding of internal control.

- *New or revamped information systems.* Significant and rapid changes in information systems can change the risk relating to internal controls.

- *Rapid growth.* Significant and rapid expansion of operations can strain controls and increase the risk of a breakdown in controls.

- *New technology.* Incorporating new technologies into service delivery or information systems may change the risk associated with internal control.

- *New activities or lines of service.* Entering into business areas or transactions with which the organization has little experience may introduce new risks associated with internal control.

- *Organization restructure (centralizing, decentralizing).* Restructuring may be accompanied by staff reductions and changes in supervision and segregation that may change risks associated with internal control.

- *Accounting pronouncements.* Adoption of new accounting principles or changing accounting principles may affect risks in preparing financial statements.

.108 Risks are potential costs or undesirable results from weaknesses. When reviewing internal controls, focus on the objective, for example, that all user charges are billed and recorded. The controls which serve to meet that objective should be identified.

.109 When evaluating a system, the strength of individual controls should be compared. How well does a particular control prevent or detect and correct errors? What does it cost? Who performs the control? Does a particular control require other controls working with it to adequately prevent errors?

.110 There may be more than one weakness causing a risk. For example, cash may be misappropriated because licenses and permits are not controlled through prenumbering and receipts are not validated on a cash register. These weaknesses together create a much larger risk than either one taken alone.

Control Activities

.111 Management should develop control activities (policies and procedures) to ensure directives are carried out and that necessary steps to address risks are taken.

Control activities should pertain to the following:

- Timely and appropriate *performance reviews*: actual to budgeted and to prior periods, financial to nonfinancial, function or activity performance.

- *Information processing* general and application controls to ensure that transactions are valid, properly authorized, and completely and accurately recorded.

- *Physical controls* for safeguarding of assets, including:

  a. Physical segregation and security of assets, protective devices and bonded or independent custodians (e.g. banks, safe deposit boxes, lock boxes, independent warehouses).

  b. Authorized access to assets and records (such as through the use of computer access codes, prenumbered forms, and required signatures on documents for the removal or disposition of assets).

  c. Periodic counting and comparison of actual assets with amounts shown in accounting records (e.g. physical counts and inspections of assets, reconciliations and user review of computer-generated reports).

- *Segregation of duties* for authorization, recordkeeping, and custody of the related assets to reduce the opportunities for any individual to be in the position to both perpetrate and conceal errors or fraud in the normal course of duties.

- *Documentation*: Internal control systems, all transactions and other significant events are to be clearly documented, and the documentation is to be readily available for examination at each agency.

  a. Documentation of internal control systems is valuable to managers in controlling their operations and may also be useful to auditors or others involved in analyzing and reviewing operations.

  b. Written evidence of (1) the internal control objectives and techniques and accountability systems, and (2) all pertinent aspects of transactions and other significant events is essential. For each agency, two written documents are recommended: a narrative on the review of internal control and an analysis of risk factors.

c. Documentation of internal control systems should appear in management directives, administrative policy, and accounting procedure manuals. Documentation of transactions and other significant events should be complete and accurate and should allow tracing the transaction or event from before it occurs, while it is in process, through its completion.

d. Many documentation tools are available such as checklists, flow charts, narratives, and software packages. Supporting documentation for conclusions should be gathered and kept on file at least five years.

Information and Communication

.112 The information system, which includes the accounting system, should provide identification, capture, and exchange of information in a timely manner.

.113 Communication should provide an understanding of individual roles and responsibilities pertaining to internal control; it should be written (policy and procedure manuals, financial reporting manuals, and memoranda), or may be oral and by example (through the actions of management).

Accounting System

.114 The accounting system should consist of the methods and records established to record, process, summarize, and report entity transactions (as well as events and conditions) to maintain accountability for the related assets, liabilities, and equity. These methods and records are to:

- Identify and record all valid transactions.
- Describe transactions in a timely manner and in sufficient detail to allow proper classification.
- Measure and record the proper monetary value of transactions.
- Determine and ensure recording of transactions and events in the proper time period.
- Present transactions and events and related disclosures properly.
- Maintain a traceable audit trail.

.115 The Oregon Department of Administrative Services (DAS), State Controller's Division (SCD) will review all proposed acquisitions, development, or modifications of **accounting systems**. See **OAM 10 65 00**, Approval of Proposed Fiscal Systems.

Monitoring

.116 Establishing and maintaining internal controls is a responsibility of management. Monitoring is the process that assesses the quality of internal control performance over time, by assessing design and operation on a timely basis and taking necessary corrective actions. The monitoring process should include ongoing activities built into regular management and supervisory activities.

.117 Agencies, at their option, should consider implementing a review process and preparing a formal report periodically on the adequacy of the agency's internal control. The report should certify the adequacy of the internal control and identify weaknesses and planned corrective actions. Agency management is responsible for follow through and appropriate actions necessary to correct identified weaknesses and risks.

OREGON ACCOUNTING MANUAL		Number 10.15.00
Oregon Department of Administrative Services State Controller's Division	**Policy**	Effective Date December 1, 2004
Chapter	**Internal Control**	.1 OF .5
Part	**Transaction Documentation Requirements**	
Section		Approval **(Signature on File at SCD)**

Authority **OAR Chapter 166**
ORS Chapter 192
ORS 291.015
ORS 293.590

Purpose and Scope

.101 This policy emphasizes the importance of internal controls related to accounting transaction documentation and how these controls help achieve reliability in financial reporting. It applies to all state agencies that record transactions in the Statewide Financial Management Application (SFMA), whether the transactions are entered directly or through an interface.

.102 This policy is intended to emphasize and strengthen those aspects of transaction documentation that generally apply to most transaction types. It is not intended to replace any of the specific documentation requirements contained in other OAM policies and procedures.

Overview

.103 The primary focus of control policies and procedures is to process transactions correctly. Transaction processing controls, including documentation requirements, should be designed with these objectives in mind:

a. Recorded transactions are valid and supported by appropriate documentation; none are fictitious.

b. All valid transactions are recorded; none are omitted.

c. Transactions are properly authorized.

d. Transaction dollar amounts are properly calculated and accurately recorded.

e. Transactions are properly classified in the accounts.

f. Transaction accounting/posting is complete; no required fields or sub-ledger entries are omitted.

g. Transactions are recorded in the proper accounting period (fiscal year).

Policy Standards

.104 All transactions must be supported by appropriate documentation. The same documentation requirements apply to transactions entered directly into SFMA, as well as those initially entered and processed in an agency subsystem that are transmitted to SFMA through an automated interface. In all cases, the documentation must be complete and accurate and must allow a transaction to be traced from the source documentation, through its processing, to the financial reports. All documentation should be readily available for examination.

.105 Records of transactions and significant accounting events may be initiated and stored in a variety of media and physical formats, including paper documents, microfilm, microfiche, magnetic tape, digital images, and other electronic and recording media. These records should be retained the minimum length of time and authorized for disposition in accordance with the requirements described in Oregon Administrative Rules, Chapter 166.

.106 Documentation requirements for accounting transactions (including records retention guidelines) should be incorporated into agency specific policies and procedures, with relevant training provided to agency personnel.

Documentary Evidence

.107 Regardless of the format used for storage purposes, all recorded transactions (including adjusting entries and transfers) should be supported by copies of source documents (such as vendor invoices, receiving records, cash receipts, timesheets, loan documents, or bank statements) and other supporting information sufficient to provide clear evidence of the following:

a. The authenticity of the transaction.

b. The purpose or reason for the transaction.

c. The vendor/customer involved in the transaction, when applicable.

d. That the transaction was properly authorized.

.108 Valid documentary evidence supports the financial statement assertions of existence or occurrence -- that assets, liabilities and equities actually exist and that revenue and expense transactions actually occurred.

Standardized Coding Information

.109 The documentary evidence must also support the information recorded in SFMA for the key data fields listed below. These fields are closely connected to the financial statement assertions of valuation (accurate transaction amounts); presentation and disclosure (proper fund, general ledger account and/or expenditure/revenue classification); existence and completeness (recorded in the proper accounting period); and rights and obligations (vendors and customers correctly identified).

a. D23 Fund and/or PCA/Index

b. General Ledger Account

c. Comptroller Object (or Agency Comptroller Object)

d. Transaction Dollar Amount

e. Vendor Name/Number, if applicable

.110 The information entered into the key data fields may be documented through the use of coding block stamps and pre-formatted input forms, or it may be hand-written directly on the source documents.

.111 For some transaction types, SFMA and agency system interfaces may be programmed to automatically "fill" one or more of the key data fields. In these situations, agencies are not required to note this information on the supporting documents, *if* it can be verified for audit purposes by reference to look-up tables, crosswalks, charts, reports, or other reference tools, such as accounting policy and procedure manuals. If the key data field information cannot be easily verified using one of these alternative methods, the information should be noted directly on the transaction documentation.

.112 Although this policy establishes the minimum documentation standards, each agency should determine what additional information needs to be documented to meet its unique business requirements and identify this additional information in its policies or procedures (referred to in paragraph .106).

System-Generated Transactions

.113 Certain transactions recorded in SFMA are automatically generated using predetermined system parameters that do not require manual data entry or manual approvals. For audit purposes, agencies should be prepared to explain the underlying logic of these transactions and to demonstrate their validity. Recurring cost allocation entries are a typical example. Documentation (which may include electronic spreadsheets) that clearly describes the methodology, the cost drivers, the formulas and calculations, and the applicable system links and processes should be maintained. In addition, copies of the initial approval documentation for these automatically generated transactions should be available for review.

Correction of Errors

.114 When a coding error in a key data field is discovered by the processing unit (e.g., the business unit entered the wrong comptroller object in the coding block), the correct information should be indicated on the document and initialed. It is not appropriate to simply enter the correct data into SFMA or an agency subsystem without making a notation of the correction on the supporting documentation.

.115 For journal entries that are specifically prepared to correct transactions that have already been processed, the supporting documentation should include a copy of the original erroneous entry (R*STARS screen print, hard-copy report, query results) or other documentation/reference that clearly indicates the origin of the error being corrected. When a copy of the original erroneous entry is included, it is not necessary to also include a copy of the supporting documentation from the original entry.

Authorization

.116 Agency heads are authorized to make expenditure decisions by statute and legislative appropriation. In addition, they may delegate expenditure decision authority to subordinates. These delegations should be evidenced by written documentation and kept current. The signed documents may be kept on file centrally in the agency Controller's Office or Business Office, or they may be filed in branch or field offices. See **OAM 10.40.00** for more details concerning delegation of expenditure authority.

Adjusting Entries and Transfer Transactions

.117 In addition to operational types of transactions (cash receipts and cash disbursements), agencies also process various kinds of transactions that are collectively referred to as adjusting entries. Adjusting entries may be recurring or non-recurring and include, for example, entries to correct errors, reclassification entries, year end accruals, and other adjustments required for financial statement purposes.

.118 All adjusting entries should be fully documented and properly authorized. In addition to source documents (see paragraph .107), the supporting records may include electronic spreadsheets, SFMA reports/screen prints, BRIO or other database queries, and agency subsystem reports/screen prints. If a database query or ad hoc report is involved, the agency should document the query/report parameters, including limits, and be prepared to explain the logic. In the case of Brio queries, for example, agencies may use the "File > Export > SQL" command which allows users to save the Structured Query Language (SQL) as a text file.

.119 When accounting estimates are used, as in the case of year end accrual entries, the rationale and underlying methodology (trend analyses, ratios, assumptions, etc.) should be documented and readily available for audit. The estimates should be reasonable and based on relevant information. The supporting records for estimates are generally not source documents (as described in paragraph .107), but rather documentation of how the estimated amount was determined.

.120 Interfund and interagency transfer transactions, including year end transfer accruals (due to/due from other funds/agencies) are subject to the same documentation requirements discussed in paragraph .118 and .119. All transfer transactions should be properly authorized and the purpose or reason for each individual transfer clearly explained in the supporting documentation.

.121 Individuals who are familiar with the related processes and have appropriate experience and background should be assigned responsibility for reviewing and approving adjusting entries and transfer transactions. For adjustments and transfers involving highly sensitive or subjective matters, such as accruals of claims and judgments, significant year end revenue and expenditure accruals, adjustments to recognize asset impairments, or other unusual items, the documentation should indicate these types of adjustments were properly reviewed and authorized.

Effective Dates and Year End Processing

.122 The supporting documentation should also provide evidence that the related transactions were recorded in the proper accounting period (fiscal year). The effective date of a transaction determines the *fiscal year* in which the transaction is recorded. Normally, cash transactions that occur during the fiscal year do not present a problem because they are recorded with effective dates prior to the close of month 12 (June). At year end, recording transactions in the proper accounting period is more complicated. Many of the non-cash adjustments required for reporting in accordance with generally accepted accounting principles should be recorded after June close. To ensure these adjustments are posted to the current fiscal year, they should be entered into SFMA as month 13 financial statement transactions, using an effective date of 06/31/YY. The supporting documentation should include sufficient information or explanation to indicate these adjustments are fiscal year end entries and that an effective date of 6/31/YY is appropriate.

.123 Many of the month 13 transactions involve expenditure and revenue accruals. The accrual entries are processed using transaction codes that automatically generate reversing entries in July of the new fiscal year. When the actual disbursements or receipts are processed in the new fiscal year, the cash transactions will be offset by the reversing entries.

Records Retention

.124 ORS 192.105(2)(a) requires each agency to designate an agency records officer who will coordinate the agency's records management and serve as a liaison with the State Archivist. The records officer should organize and coordinate records scheduling, retirement, storage and destruction. The State Archivist will provide records officers with training and assistance.

.125 Each agency is required to develop a formal records retention program in accordance with Chapter 166, Division 30 of the Oregon Administrative Rules (OAR). OAR Chapter 166 also provides technical specifications, quality control guidelines and security measures for appropriate use of microfilm, digital imaging systems, electronic records and other media.

.126 It is each agency's responsibility to review its programs and functions to ensure archive requirements are followed. This process includes identifying the specific records that should be retained and assigning ownership and custodial responsibilities for the official "record copy." Transaction documentation files should be centralized to the extent possible and readily accessible to authorized agency staff and auditors.

.127 State agencies should destroy financial records which have met the terms and conditions of their scheduled retention period, subject to the prior audit requirements of OAR 166-030-0045: "Public records of fiscal transactions, regardless of medium or physical format, may not be destroyed until the minimum retention period has passed and the person charged with their audit has released them for destruction. If federal funds are involved, requirements of the United States government shall be observed."

OREGON ACCOUNTING MANUAL		Number 10.20.00.PO
Oregon Department of Administrative Services State Controller's Division	**Policy**	Effective Date July 1, 2001
Chapter **Internal Control**		.1 OF .2
Part **Cash**		
Section		Approval Signature on file at SCD

Authority **ORS 291.001**
ORS 291.015
ORS 293.180
ORS 293.265

.101 The principle of accountability, insofar as it relates to cash on hand and bank accounts, can best be described as follows: the custodian of every cash fund is responsible for the integrity of the cash fund and his/her discharge of that responsibility is to be reviewed periodically. For **petty cash**, **change funds**, and cash receipts, this review consists of surprise counts by independent employees. For bank accounts, it consists of an independent reconciliation of the agency cash balances. The designation of specific responsibility for custody of cash funds is vitally important, and should be done through organization charts, operating manuals, position descriptions, or similar written documents.

.102 All officers and employees who have access to cash and/or are accountable for property of the State or held by the State in trust for others should have adequate surety coverage. It may be appropriate to conduct a background check on prospective employees. In the State, all officers and employees, whether classified, elected or appointed, have blanket faithful performance coverage through a bond obtained by the Risk Management Division, Department of Administrative Services. Risk Management keeps a master policy on file and available for inspection and invoices each agency for its proportionate share of the premium. However, certain inappropriate action by a State employee may negate this insurance protection for him/her.

.103 Controls and safeguards must be adequate to provide management with a reasonable degree of assurance that cash and cash related transactions will be properly accounted for and controlled.

Treasury and Bank Accounts

.104 The Treasury, in consultation with the Department of Administrative Services, may establish or designate accounts and funds as legally authorized. Most cash accounts and funds are established by specific statutes or in the Oregon Constitution. Accounts and funds shall be administered in accordance with written directive or policy issued or approved by the State Treasurer. These accounts and funds may be established whenever necessary or convenient to the carrying out of accounting, budget preparation, cash management, financial management, financial reporting or similar laws. The cash accounts and funds must also be set up in the Statewide Financial Management System.

.105 When money is received by an agency, it is deposited at the bank. With some exceptions, the State Treasurer does not allow a State agency to have an account at a bank. Instead, the agency's account is at Treasury. When agencies deposit money at the bank, they are actually depositing to the Treasurer's account at the bank. In effect, Treasury is the agency's bank and

has contracted with various commercial banks to accept deposits from agencies as a mechanism for agencies to efficiently deposit money to their accounts at Treasury.

Petty Cash

.106 An agency may establish a petty cash fund with legislative approval. The fund can only be established from legally authorized appropriations or limitations. (See ORS 293.180.)

Change Funds

.107 An agency may establish change funds without legislative or Department of Administrative Services (DAS) approval. A change fund so established is subject to periodic audit by the Secretary of State Audits Division.

Authority **ORS 291.015**
ORS 293.180
ORS 293.265
ORS 293.295
ORS 293.306
ORS 293.525

.101 As a part of the required internal control documentation, each **agency** having the power to collect State moneys should design and document internal controls for cash. The written procedures, often located in an operations manual, describe the duties of employees who handle cash. These procedures establish and document the flow of cash, cash documents, controls over cash, and the recording of cash transactions. Use of a flow chart to complement the narrative is encouraged.

.102 Collections, cashiering (deposits), bank reconciliation, and recording of accounts receivable are to be segregated to the extent possible so that accuracy and completeness can be verified through independent checks.

Deposit Reconciliation

.103 The reconciliation of bank statements is important for satisfactory control. It serves as a periodic reconciliation of existing assets to recorded amounts. The reconciliation should be done by someone not otherwise responsible for handling cash or cash records and should be reviewed by management.

.104 Reconciliations should be performed between agency records and bank or trustee statements for accounts maintained by banks or trustees and between agency records and Treasury statements for funds maintained by the Treasury.

.105 A written record of the reconciliation with Treasury or the bank, including a listing of outstanding checks and in-transit deposits should be prepared by the reconciliation accountant and retained with the statements. **Statewide Financial Management Services (SFMS)** prepares a number of reports to facilitate reconciliations from the **Relational Standard Accounting and Reporting System (R*STARS)** to Treasury, e.g. DAFR 737-3, which is distributed monthly to the agencies by SFMS.

.106 Deposit reconciliation is also mandated for all receipted accounts by SFMS. Deposits, including incoming Electronic Funds Transfers (EFTs) are not available cash in R*STARS until the deposits are reconciled. This means the deposits recognized at the bank and at Oregon State Treasury (OST) are interfaced from OST's system to R*STARS. These interfaced transactions are matched with R*STARS recorded entries. Once electronically matched, a transaction code

generates, which effects cash available for expenditure. Deposit reconcilation is addressed in the Trea1 chapter of the SFMS desk manual at http://www.oregon.gov/das/Financial/AcctgSys/Pages/deskmanual.aspx

Receipted Accounts

.107 The statements received from OST or other authorized bank (including fiscal agents or trustees) should be delivered directly to and reconciled by an employee who is not responsible for the receipt or deposit of cash, the disbursement of cash, or the maintenance of the applicable accounting records.

.108 The entries on the statement should be compared with the dates and amounts recorded by the agency.

.109 An accounting of the numerical sequence of deposits and a list of in-transit deposits should be prepared.

.110 The transaction details for checks outstanding for more than one reconciliation period should be investigated. DAS requires warrants and checks be expired if not presented for payment within two years from the date of issuance.

Suspense Accounts

.111 For agencies using suspense accounts and those not interfaced with R*STARS, the total of the paid checks returned should be proved against the charges on the bank statement. (For information on recording suspense account information in R*STARS, please refer to the Trea5 chapter of the SFMS desk manual at http://www.oregon.gov/das/Financial/AcctgSys/Pages/deskmanual.aspx.)

a. An accounting should be made of the numerical sequence of the checks and deposits.

b. All voided checks should be examined. Such checks should be retained in the numeric file of checks when checks are returned by the bank or Treasury. If checks are not returned by the bank, the voided checks should be filed with the cash disbursement records.

c. If checks are returned, the signatures and endorsements on the checks should be reviewed on a test basis by the reconciliation staff to be sure they are reasonable and complete.

d. Checks may be returned by the post office as undeliverable. Strict control should be maintained over such checks. The checks should be delivered by the mail room to an employee responsible for their control. This employee should not have access to the undeposited receipts of the agency. Reasonable efforts should be made to locate the payees. If unsuccessful, then the checks should be marked VOID and kept on file as outstanding checks until they can be expired.

General Fund

.112 SFMS Operations prepares reconciliations of the General Fund and the Lottery Fund at Treasury to the transactions in R*STARS for each accounting month. Outstanding reconciling items are researched and cleared on a statewide basis. Thus, agencies do not need to reconcile cash funds that are part of the legal General Fund or the Lottery Fund. However, agencies are responsible for investigating and clearing reconciling items when notified of them by SFMS Operations.

Cash Management Improvement Act (CMIA)

.113 Accurate cash clearance patterns are required under the federal Cash Management Improvement Act (CMIA). Also, **Generally Accepted Accounting Principles (GAAP)** require that the passage of time between an accounting event and complete recording of that event be minimized.

.114 If a temporary account or fund such as a clearing account or revolving suspense account is used to account initially for an accounting event, the elapsed time between the initial accounting transaction and the subsequent accounting transaction to clear the temporary account and reclassify the accounting event should be minimized.

Cash Receipts

.115 The term cash receipts includes receipts from all sources. It includes wire transfers and transfers in of cash, such as transfers to a cash account from another cash account in the same agency.

.116 Cash lost before being receipted is more difficult to trace than cash received and recorded. It is imperative that cash receipts and transfers be recorded as soon as they come within the agency's control. Checks are to be restrictively endorsed at the time of collection. Processing of cash receipts should be centralized to the extent workable.

.117 Cash transfers should be recorded by someone other than the cashier who is responsible for regular cash receipts. Also, the individual recording cash transfers should have no further access to cash handling or accounting.

.118 In addition, all cash received by an agency should be reconciled daily with the daily cash reports prepared from pre-numbered receipts, licenses, or permits, cash register tapes, mail room tabulations, and similar documents.

.119 Disbursements from cash receipts should not be permitted. Any cash shortage or overage should be accounted for, by employee, and should be investigated if material in amount or if a pattern is visible. Unusual items should be adequately documented and explained. ORS 297.120 requires any cash shortages from or suspected to be from employee dishonesty to be promptly reported in writing to the Secretary of State, Audits Division.

.120 The initial record of cash received may be a pre-numbered receipt form; a summary of pre-numbered license tickets or permits issued; a cash register tape; a mail room listing; or some other remittance advice, depending on the type of agency and the nature of its revenues. Some agencies use a validation machine to assign control numbers to documents.

.121 The correspondence accompanying the remittances should be stamped with the date received, and the payment data recorded thereon. These documents should then be forwarded to accounts receivable or to the accounting office and/or appropriate operating units of the agency.

.122 Remittances for which proper distribution cannot be determined should be listed separately.

.123 The fundamental rules for attaining control over cash receipts include:

a. Establish control over cash receipts immediately. Restrictive endorsements should be made on all checks as they are received.

b. Deposit each day's cash receipts intact even if proper disposition of receipt is unknown.

c. Deposit cash receipts daily (not later than one business day after receipt per ORS 293.265). Deposits of small amounts of cash can be less frequent, but must be at least weekly; however, if deposits are made less frequent than daily, the agency still needs to comply with ORS 293.265. In accordance with ORS 293.265, an agency may use a reasonable, longer period of time (other than one business day) for deposit of specific receipts if the agency

documents that a valid business reason exists for using a longer period of time and and that the period of time is no longer than necessary to satisfy the business reason, and the agency submits a copy of such documentation to the Audits Division for review. In addition, Oregon State Treasury policy No. 02 18 01 PO requires a copy of such documentation to be filed with Treasury's Finance Division.

d. Separate cash handling from record keeping. Separate billing from cash collection. (Separation may not be possible for small agencies, boards and commissions.)

e. Do not allow any one person to handle a cash transaction from beginning to end.

f. Change passwords for access to automated accounting records periodically and do not permit shared passwords.

g. Centralize receiving of cash to the extent possible.

h. Locate cash registers so customers can observe amounts as they are recorded.

i. Assign prompt reconciliation of State Treasury accounts and other authorized bank accounts to individuals not responsible for handling cash.

j. Secure cash at all times.

Mail Receipts

.124 In many agencies, most receipts are received in the mail. Mail containing remittances should be opened at designated times, usually once or twice a day, by two designated persons. In cases of extremely heavy periods of incoming mail, it may be necessary to open the mail throughout one or more daily shifts by large numbers of personnel. In cases where the volume of receipts is light and/or the cash received is in small amounts and risk evaluation indicates low risk levels, one person may open the mail. If only one person opens the mail, additional control procedures may be required, such as adequate supervision, test checks of receipts and deposits, and periodic reassignment of duties.

.125 If several types of revenues are received simultaneously, the documents received from payors should be sorted by type. This can be done by using a bank lockbox or separate post office boxes.

Receipt Forms

.126 The fundamental purpose of the serially pre-numbered receipt form is the control of currency collections. Receipts should be issued for all currency collections regardless of source. Normally, receipt forms would not be used when recording noncurrency items where other controls are adequate. However, receipt forms should provide for indicating the purpose and type of money received (currency, check, money order).

.127 Where it is necessary to initially record receipts at different locations, the receipt form may be used as a subsidiary cashbook. In such cases, all receipts including currency, money orders, and similar items should be entered in the pre-numbered receipt book.

.128 To assure maximum potential control over cash receipts from the use of pre-numbered receipt forms, the following procedures should be followed:

a. The forms should be pre-numbered and printed in triplicate. When prepared, the original is given to the person from whom the cash is received; the duplicate is used to establish accountability for the cash collected and the triplicate is retained in numerical sequence to establish accountability for the forms used. The original should be clearly differentiated from

the copies by color or with the word “COPY” displayed prominently on the duplicate and triplicate.

b. When it is necessary to void or cancel a receipt form, the original should be marked void so it cannot be reused, and the original should be attached to the duplicate and triplicate and should be retained.

c. A listing of the quantities of forms delivered and the numbers thereon obtained from the printer provides a basis for perpetual inventory control over the forms available for use and reconciliation of issued forms. The inventory and custody of forms should be segregated from the cashiering function and accounting records for cash. The book inventory should be periodically verified against the actual forms on hand by an individual other than the one maintaining the record.

Automated Collection Methods

Cash Registers

.129 There are two separate objectives regarding control of receipts collected through the use of a UPS code scanner or a cash register: (1) to assure all cash collected is recorded on the register, and (2) to assure all cash recorded on the register is accounted for and turned over to the designated employee for deposit. Some degree of assurance can be provided through certain techniques. For example, cash register sales of certain commodities can be controlled by keeping a perpetual inventory at “retail” value on the merchandise available for sale. Physical inventories are taken periodically, and the cashier should account for the value of the book inventory under his/her control either in physical stock on hand or cash collected.

.130 Control can also be provided by positioning the cash register so that amounts recorded on the register are obviously displayed to the customers and customers are provided with receipts for their transactions. An additional control technique employs “spotters”, unknown to the cashier, to periodically observe the cashiering function.

.131 The register should be equipped with a tape on which cash collected is listed and accumulated. To determine that all register tapes are accounted for:

a. Control should be maintained over all cash registers by manufacturer’s number, or other suitable means, to preclude substitution or use of cash registers not authorized.

b. The cumulative total on each register should be locked by a service technician so it cannot be cleared and turned back.

c. If transaction numbers cannot be turned back and are printed on the tape, assurance is provided when the first transaction number on each tape consecutively follows the last number on the previous tape.

.132 An individual other than the register cashier should count the cash and extract the register tape in the cashier’s presence. The amount collected should be balanced with the register total, as shown by the tape or the cumulative locked-in totals. All register tapes and reports and readings should be collected by someone independent of the collection process and retained chronologically in a file.

Validation Machines

.133 Some agencies use a validation machine to account for and control cash receipts. This machine prints a number on the check received, and prepares a corresponding list of receipts showing the number assigned, the date, and the amount. The validation machine is normally operated by an individual who is not part of the accounting staff.

Prelisting

.134 Each cash transmittal should be accompanied by the corresponding duplicate copies of the prenumbered receipts issued or the validation machine tape and a cover document (prelisting) identifying the dollar amount, sequence of receipt numbers transmitted, and the period of time covered by the transmittal. The prelisting is prepared in as many copies as required. The original and copies should be forwarded, together with the remittances, to the cashier for deposit.

Deposits

.135 Moneys received should be turned over to a designated cashier for deposit at prescribed intervals. If possible, this transmittal should be made within one business day of receipt. If daily transmittal is not feasible due to location of collection or other business reasons, or if amounts of collections are nominal, transmittals may be made less frequently, but should not be less frequently than once a week. If deposits are made less frequent than daily, the agency needs to comply with ORS 293.265. In accordance with ORS 293.265, an agency may use a reasonable, longer period of time (other than one business day) for deposit of specific receipts if the agency documents that a valid business reason exits for using a longer period of time and that the period of time is no longer than necessary to satisfy the business reason, and the agency submits a copy of such documentation to the Audits Division for review. In addition, Oregon State Treasury policy No. 02 18 01 PO requires a copy of such documentation to be filed with Treasury's Finance Division.

.136 A specific exception to the statutory requirement of depositing all receipts to a State Treasury account is that a State agency may return any bank check whenever such bank check or money order is incomplete or the report or record applied for is not available or releasable or the payment is not owed. The agency shall keep a record of the check or money order returned.

Electronic Funds Transfer (EFT)

.137 Electronic Funds Transfer (EFT) usually means transfer through the Automated Clearing House (ACH) or the Federal Reserve's Fedwire system. EFT's offer a number of control advantages over paper-based systems. An EFT system generally has various levels of security, which may include encryption of data, authentication of transaction accuracy, and secured access to facilities. There is no paper item to be lost in the mail or stolen from the mailbox. There is no need to go to the bank to make a deposit.

.138 Agencies should work with the Oregon State Treasury (OST) to determine the best method available to take advantage of the opportunities of the ACH system. For additional details and required forms, see the OST's Cash Management Manual at their web site at http://www.oregon.gov/treasury/Divisions/Finance/StateAgencies/Pages/Cash-Management-Manual.aspx.

Cash Disbursements

.139 Where segregation of duties cannot meet optimum, the control requirement should provide as much separation as possible between the responsibilities for: originating requisitions; placing orders; reporting receipts; and approving invoices for payment.

.140 All disbursements, except those using electronic funds transfer or from non-bank petty cash funds should be made by check or warrant.

.141 Agencies should process vouchers on a timely basis (within 45 days for most vendors, within 30 days for construction vendors) to avoid paying interest on accounts, as required by statute. For cash management purposes, however, payments should not be made too soon so that the State can maximize interest earnings.

.142 The following standards should be applied in prescribing procedures for handling cash disbursements in the agency:

a. An agency policy and procedure manual should be developed to describe the authority and responsibility for expenditures in accordance with State policies and procedures.

b. The functions of approving vouchers, preparing checks, and recording disbursements should be handled by different employees. Employees handling disbursements should not have duties relating to cash receipts or the reconciliation of bank accounts.

c. Payment should be made or vouchers prepared only after the original and all copies of pertinent papers have been approved. Payment should only be made from original invoices, or in limited and unusual situations, from original statements.

d. Vouchers or checks should be approved or signed only on presentation of satisfactory documentary evidence that disbursement is properly authorized.

e. Invoices and, if applicable, statements should be canceled or stamped in a prescribed manner in order to preclude reuse of the documents.

f. A periodic review of the documentation supporting payments should be made by an authorized person to assure all processing steps and approvals are being properly applied.

Checks and Warrants

.143 All agencies drawing checks and warrants on State Treasurer's accounts will use the single State check design. The single State check utilizes a controlled paper stock with numerous security features and a background design that makes all State checks and warrants easily recognizable as State items. Instructions for ordering can be found at OST's web site: http://www.oregon.gov/treasury/Divisions/Finance/StateAgencies/Pages/Cash-Management-Manual.aspx.

.144 As a protection against misuse or alteration, care should be exercised in preparing checks and warrants. Written and figure amounts should be inserted far to the left in prescribed spaces to avoid the possibility of a later insertion in front of the correct figure. Checks should never be drawn to bearer or cash.

a. A limited number of persons should be authorized to sign checks and/or warrants and the signatures of these persons should be on file.

b. The supporting vouchers and documents should accompany the checks when submitted for signature. These documents should be examined before signatures are affixed. The documents should bear the prescribed approvals, showing compliance with purchasing, receiving, and payment procedures.

c. Signature cards, properly approved, should be on file for those employees authorized to approve documents, such as purchase orders and vouchers, and receiving reports. For agencies using electronic approvals, these documentation controls are essential.

d. Checks should not be distributed or mailed by the same employee who prepares the checks if he/she has access to the applicable records.

e. When dual signatures are required on checks, the two employees authorized to sign checks should be administratively independent of each other. Rubber stamps should not be use for check signing.

f. Check signing machines and laser signatures should not be used, except in cases where a large volume of checks are processed. When they are used, the signature plates should be

kept in the custody of the officials authorized to sign checks or their authorized representatives. Although the use of the machine relieves the officials of the manual signing operation, these officials will still be held responsible for an examination of the supporting documentation. If two signatures are required, a separate signature plate should be used for each signature.

g. Check signing machines usually provide registers to control either or both the number of checks signed and the total amount processed through the machine. These control totals should be reconciled daily with the recorded cash disbursements.

h. When it is necessary to void a check, it should be marked "VOID" and the signature space crossed out. All voided checks should be filed numerically with the paid checks returned by the bank and kept by the agency. If checks are not returned by the bank, the voided checks should be filed with the cash disbursement records.

i. The number of pre-numbered checks purchased should be supported by a listing from the printer as to the quantity shipped and the check numbers included in the shipment. Unused check stock should be kept in a locked or otherwise secure area. All check numbers should be accounted for by someone lacking access and responsibility for check stock and check issuance.

j. All checks written should be entered in numerical order in a cash disbursements journal or other cash disbursement record. Separate disbursement records should be kept for each checking account. With an automated cash disbursement system, the computer should generate an appropriate cash disbursement record.

Petty Cash and Change Funds

.145 Each agency with a **petty cash** fund and/or **change fund** must develop its own written operating and reconciliation procedures.

.146 Petty cash funds must be maintained on an imprest basis, meaning each fund will be replenished for the exact amount of the expenditures made from the fund. The fund must be replenished as required to maintain cash at the authorized level.

.147 A custodian of a petty cash fund must be designated as responsible to account for and service the fund. The custodian can use petty cash to reimburse claims approved by persons designated to approve cash payments from the fund. For claim reimbursement, there must be a valid receipt and signature approval for purchase.

.148 Change funds must meet a specific business need such as currency and coin needed to provide customer purchase convenience or special program related circumstances. Change funds are to be kept at the minimum level necessary to handle normal customer service needs.

.149 An employee must be designated to be responsible for the agency change funds. If change funds are further distributed to individual employees, each person is responsible for the change fund so entrusted.

.150 The amount of each change fund remains constant, and that amount should be withheld at the close of each day from the total cash in the register or cash drawer as the funds with which to begin the following day. The remaining cash is recorded as the current day's receipts and is reconciled to the receipt documents.

.151 At a minimum, the following internal controls over petty cash and agency change funds must be established:

a. If the agency maintains a change fund in addition to a petty cash fund, the two funds must be kept separate and not be commingled.

b. Secure physical cash at all times.

c. Conduct periodic unannounced counts by an independent employee not the petty cash custodian or change fund cashier.

d. The petty cash custodian must not be authorized to approve cash payments from the fund or to authorize replenishment of the fund.

e. Personal checks are not allowed to be cashed from agency cash funds.

f. All disbursements from the petty cash fund should be supported by invoices and vouchers properly approved and dated. These documents should be examined and canceled when the fund is reimbursed.

g. The accounting section in the agency should keep a record of the amount of each change fund and its location. Each fund custodian must provide a signed receipt to establish accountability for the change fund entrusted to him/her. The receipts are to be kept on file in accounting.

h. Daily cash receipts from business transactions should be deposited and should not be retained in the change fund after the close of the business day.

i. Update policies and procedures as needed and ensure compliance.

j. Periodically evaluate each petty cash and change fund as to need and size. To the extent possible, eliminate petty cash and change funds.

Postage

.152 Controls over postage can be most effectively established through the use of a postage meter. All metered postage should be purchased by check or warrant, payable to the postmaster. An employee independent of the mailroom should verify the amount entered on the meter is the full amount of the check or warrant. Under no circumstances should checks or warrants issued for metered postage be used for the purchase of stamps or exchanged for cash.

.153 The postmaster's receipts for metered postage should be retained and a daily record be kept of the meter readings; at intervals, the changes in the ascending and descending meter readings should be reconciled with metered postage purchases for the period.

.154 Special circumstances may require the use of postage stamps. This practice should be kept to a minimum and controlled by the use of requisitions. The stamps should be purchased by check. A single individual should be responsible for the distribution of the stamps and should maintain a record of receipt and distribution. At intervals, the stamps in custody of this individual should be inventoried and reconciled with the stamps purchased and requistions filled. The reconciliation should be performed by a staff other than the individual with custody of the stamps.

Authority **ORS 291.015**
ORS 293.590

Revenue Controls

.101 Management must establish and maintain adequate internal controls over revenue. At a minimum, these controls should provide evidence of the following:

a. Revenue transactions occurred and that cash and revenue amounts exist as recorded.

b. All revenue transactions are recorded and nothing has been excluded from the accounts.

c. Revenue is properly classified as to source, mathematically correct, and entered appropriately into the accounting system. Restricted revenue is classified separately to show restricted rights and obligations.

d. Revenue is recognized in the proper period, neither postponing current period recordings to the next period nor accelerating next-period transactions into the current-year accounts.

e. Revenue transactions are reported in accordance with accounting principles and in compliance with applicable legal, administrative, and budget requirements.

Accounts Receivable

.102 Recording uncollected revenues (revenues earned but not received) results in the recognition of receivables. Receivables include loans, notes or similar obligations owed to the agency and must be recorded in the accounting records. Accounts receivable generally arise from the sale of goods or the rendering of services, but accounts receivable also arise from other sources, such as overpayments of entitlements. Accounts receivable include the amounts due for goods and services provided by state agencies to other state agencies, local governments, nonprofit organizations, and others.

.103 Adequate internal control over receivables must be established and maintained. Adequate controls must include, at a minimum: separation of duties or appropriate compensating controls, proper authorization of transactions, and timely reconciliations. Collection documentation will include a record indicating the action taken, person performing the action, and the date of the action. Collection documentation must also include summaries of collection efforts and results, summary totals of accounts written off, and results of using other collection expertise.

Documentation should also include other information deemed necessary to aid in identifying effective collection programs and areas that need improvement. A cumulative history can aid in the improvement of receivables management and collections.

.104 Accounts receivable will be aged and analyzed. The analysis will be documented and will include, at a minimum, the aging of accounts receivable balances, descriptions and summaries of payees or debtors and evaluation of the quality of the accounts receivable for management review and appropriate action.

.105 Refer to Oregon Accounting Manual Chapter 35, Accounts Receivable Management, for details regarding Liquidated and Delinquent Accounts, as well as Interagency Receivables, Billings, and Payments.

Authority **ORS 291.015**
ORS 293.590

Revenue Controls

.101 Separation of duties is a primary revenue control. Only specifically authorized individuals should be responsible for collection and recording of revenue. No one person should handle a revenue transaction from beginning to end. Ideally, an individual should not be responsible for recording both revenue and expenditure transactions. If separation is not possible, compensating controls including periodic independent reviews as appropriate with respect to timing of the revenue stream must be in place. Such independent checks should be performed by management or external parties.

.102 Management should assure timely reconciliation of subsidiary accounts to control accounts and provide adequate review and approval of reconciliation documentation.

.103 Managers should compare revenue accounts and amounts to prior-year data and to multiple-year trends to ascertain whether any unusual fluctuations are present. Comparisons should be made to budgets, monthly internal reports and forecasts to determine whether events have occurred that require explanation or analysis by management.

.104 The best control over revenue is control over the source of the revenue. Four examples are:

a. Accounting control over merchandise inventory, including periodic physical inventories by an individual who does not maintain the inventory, provides the best assurance that all sales of merchandise are recorded. In this regard, the inventory account should be credited only for recorded sales transactions. All credits to the inventory control account other than sales transactions should be reviewed by the internal auditor, if applicable, or the chief financial officer.

b. Control over service hours provides the best assurance that an accounting has been made for all sales of services on an hourly basis. In this regard, service hours should be controlled until they are either billed or written off by an authorized person.

c. Some types of revenue are controlled by the issuance of serially numbered licenses, permits, tickets, food stamps, and similar items which provides an accountability over the revenues collected. Periodically, at least annually, the number of licenses and similar items issued should be reconciled with the number available for issuance and the revenues collected. A perpetual inventory of licenses, permits and similar items is recommended.

d. For day-to-day revenue streams, there are special mechanisms in use which afford revenue accountability. These include treadle, turnstile and other meters which independently record the number of customers serviced. Readings from these control devices should be reconciled daily with collections by an individual not responsible for collections.

Deposits

.105 In some agencies, deposits are required for various purposes, such as for rental of equipment, dormitory room deposits, pre-registration deposits, and contractors' bid deposits. Records should be established to record the receipt and disposition of such deposits. In most cases, subsidiary records are required to show the name of payors to whom individual deposits will be refunded or credited. Periodically, but not less than annually, the total of the balances of subsidiary records should be reconciled with the deposit account.

Receivables

.106 Internal controls over receivables should provide for a proper division of functional responsibility. Proper division exists when all amounts entered in the receivable control account originate in sections or units other than the receivables section. Smaller agencies may have to rely on compensating controls. Debits should be transmitted from the billing section and credits for cash receipts from the cashier. Management should divide the functions in such a way that all non-cash credits to receivables are controlled by an officer or responsible employee who does not have access to or authority over the cash books. All non-cash credits to customers' accounts should be authorized by the chief financial officer or other accounting manager not responsible for recording the credits.

.107 Invoices received from the billing section should be accompanied by the total amount of the invoices presented. If this is not done, a tape should be run in the receivables section so that the total posting may be proved against this pre-run total. There should be a daily proof of all postings against the entries in the control account.

.108 Information with respect to cash receipts should come from the cashier in the form of a list of receipts or, in larger organizations where total receivables necessitate, in the form of a remittance advice. A pre-run total should be obtained to act as a proof against the sum of the credits posted to the receivable account.

.109 Regular monthly balancing of the subsidiary ledgers with the control account by an independent person is an essential internal control. Without this monthly reconciliation, errors are more difficult to locate. Monthly reconciliation isolates any error on a timely basis and thus reduces the time necessary for identification and correction. Reconciling items should be promptly resolved.

.110 Monthly statements should be prepared and mailed early in the month. This task should be done by some person independent of the cashier, credit, or receivables section. Where the statements are prepared as a part of the posting process, an independent person should check the original statement against the ledger. The control over these statements should be such that any undeliverable statement and any complaints received about the statement should be channeled to the person who prepared or checked the statements and mailed them, not the receivables accountant. The control comes from separating the statement from the person who is responsible for the original postings of receivables.

.111 Refer to Oregon Accounting Manual Chapter 35, Accounts Receivable Management, for details regarding Liquidated and Delinquent Accounts as well as Interagency Receivables, Billings, and Payments.

OREGON ACCOUNTING MANUAL

Subject:	Accounting and Financial Reporting	Number:	10.35.00.PO
Division:	State Controller's Division	Effective date:	April 17, 2008
Chapter:	**Internal Control**		
Part:	**Credit Card Acceptance for Payment**		
Section:			
Approved:	John Radford, State Controller	Signature on file at SCD	

Authority **ORS 291.015**
ORS 291.026
ORS 293.265
ORS 293.590

Authorization

.101 State agencies must make application to and be preapproved by the Office of the State Treasurer (OST) to accept credit cards in payment of products, services and other fees. In addition, third party service organizations that provide storage, processing, or transmission services and/or applications to state agencies associated with credit card transactions must be prequalified by OST.

Agency Responsibilities

.102 State agencies authorized by OST to accept credit card payments must:

a. Establish a system of internal control that provides reasonable assurance that all credit card transactions are properly authorized, timely settled, and accurately and completely recorded. In addition, controls and safeguards must be established and maintained to reduce the risk of unauthorized access and to monitor for errors, both unintentional and intentional errors, including fraud.

b. Ensure that all employees responsible for accepting and processing credit card payments receive appropriate training and are familiar with and have access to US Bank Merchant Terms of Services (MTOS) and Discover Business Services Merchant Operating Regulations (MOR). Training is available through OST.

c. Ensure that personnel involved in accepting and processing credit card payments do not use, disclose, or disseminate cardholder information except for the purposes of processing the associated financial transactions.

d. Comply with MTOS/MOR; all applicable OST requirements; payment card industry security standards; statewide IT security policies and initiatives issued by the Department of Administrative Services, Enterprise Information Strategy and Policy Division (DAS-EISPD); and all federal and state laws pertaining to safeguarding personal information and notifying consumers in the event of a security breach, including the Oregon Identity Theft Prevention Act (Oregon Laws 2007, Chapter 759).

OREGON ACCOUNTING MANUAL

Subject:	Accounting and Financial Reporting	Number:	10.35.00.PR
Division:	State Controller's Division	Effective date:	April 17, 2008
Chapter:	**Internal Control**		
Part:	**Credit Card Acceptance for Payment**		
Section:			
Approved:	John Radford, State Controller	Signature on file at SCD	

Purpose and Scope

.101 This procedure describes internal controls and safeguards that must be implemented to:

a. Provide reasonable assurance that all credit card transactions are properly authorized, timely settled, and accurately and completely recorded;

b. Reduce the risk of unauthorized access and to monitor for errors, both unintentional and intentional errors, including fraud;

c. Protect the security, confidentiality and integrity of cardholder information; and

d. Comply with notification requirements in the event of a security breach.

.102 The requirements set forth in this procedure apply to all state agencies that process credit card transactions. Each agency that accepts payments by credit cards has a responsibility to understand the unique issues of operating its e-commerce program and to create internal policies and procedures to address those issues. Agencies are encouraged to contact the Office of the State Treasurer (OST) and the State Controller's Division (SCD) to learn more about the various tools and controls available to reduce exposure to e-commerce risks and minimize the associated losses. OST can also advise agencies on ways to process credit card transactions that will increase efficiency and reduce transaction fees.

.103 None of the controls described below relieves agencies of their responsibility to comply with policies published by OST, the US Bank Merchant Terms of Service (MTOS) or Discover Business Services Merchant Operating Regulations (MOR). Agencies must adhere to OST policies and the MTOS/MOR. When credit card fraud is suspected, for example, agencies must refer to the MTOS/MOR guidelines.

Point of Sale (POS) Transactions – Control Requirements

.104 Agencies that accept and process credit cards in payment of products, services, licenses, or other fees in face-to-face transactions conducted over the counter must incorporate the following control procedures into their operations.

a. Before swiping the customer's credit card through the POS terminal, verify that the card expiration date has not passed. **Expired credit cards must not be accepted for payment.**

b. Ensure that the dollar amount charged to the card is fixed by the transaction. **No cash refund or credit may be issued in conjunction with the purchase transaction.**

c. If the authorization network approves the transaction, ask the customer to sign the sales receipt and then compare the customer's signature with the signature on the back panel of the credit card. **Unsigned cards must not be accepted.**

d. Compare the name and account number on the credit card with the name and last four digits of the account number on the printed receipt. **Refer to the MTOS/MOR if the name or digits do not match.**

   NOTE: The MTOS/MOR requirement that all POS devices must suppress all but the last four digits of the credit card account number and the entire expiration date on the cardholder's copy of the transaction receipt is consistent with Oregon law. The Oregon Identity Theft Prevention Act (Oregon Laws 2007, Chapter 759) states that data shall be redacted so that no more than the last four digits of a customer's credit or debit card number are accessible.

e. If the credit card's magnetic stripe cannot be read, and the cardholder's information is key-entered, agencies must:

   - Request Address Verification Services (AVS).
   - Make a physical imprint of the card using a manual imprinter.
   - Obtain the cardholder's signature on the imprinted transaction receipt and compare it to the signature on the back panel of the card. **Unsigned cards must not be accepted.**
   - Black-out all but the last four digits of the credit card number on the cardholder's copy of the receipt.

f. To complete the transaction, information necessary for the delivery of purchased goods or services may be requested and recorded as long as the information is provided voluntarily by the credit cardholder (**ORS 646A.214**).

.105 If a "declined" or "no match" response is received from the authorization network, the credit card cannot be accepted. Agencies shall offer to process a different, valid credit card or another acceptable form of payment, such as a personal check or cash.

Telephone and Mail Order Transactions – Control Requirements

.106 Agencies that accept and process credit cards in payment of products, services, licenses, or other fees in transactions that are conducted by telephone or mail order must incorporate the following controls into their operations.

a. Request Address Verification Services (AVS).

b. Ensure that the transaction documentation includes the agency's order number (e.g., invoice number, license number or similar identifier) and the agency's customer service number.

Internet Transactions – Control Requirements

.107 Agencies that accept and process credit cards in payment of products, services, licenses, or other fees in transactions that are conducted over the Internet must incorporate these additional controls into their operations.

a. If products and/or services have a fixed fee, the system must populate the amount field based on the customer's selection.

b. The Internet website must incorporate fraud prevention measures, such as Address Verification Services (AVS), Card Verification Value (CVV2), Card Validation Code (CVC2), or other fraud prevention tools available through the issuing bank. Refer to the MTOS/MOR for further information.

Fulfillment and Revenue Recognition

.108 Unless the agency and merchant bank have agreed otherwise and such agreement is in writing, any agency accepting payment by credit card must place a "hold" on the order through the payment processing system, if the product or service is not available for immediate shipment or fulfillment. (This rule applies to all methods of processing credit card payments, including over-the-counter transactions, telephone and mail orders, and Internet transactions.) The "hold" shall be released when the order is shipped or fulfilled. The settlement date may not be more than seven (7) days from the authorization date.

.109 Under generally accepted accounting principles (GAAP), credit card "sales" revenue is recognized when the customer's order has been fulfilled or shipped and the exchange is completed. Credit card revenues associated with licenses and fees are recognized upon receipt. For more information on revenue recognition, refer to **OAM 15.35.00**, Revenues and Receivables.

Deposit/Settlement

.110 Unless an exception is received by the agency, all credit card transactions must meet the deposit requirements of **ORS 293.265**.

.111 Credit card terminals: The daily receipts totals from all credit card processing devices must be printed and used to settle transactions at the end of each business day. Transactions settled before 5:00 p.m. will be posted to the agency's account at OST at midnight.

.112 DAS SecurePay or other payment processor: Daily transaction batches must be submitted before 5:00 p.m.

.113 Transactions settled before 5 p.m. will be posted to agency accounts the next business day if there are no changes/errors in the normal daily processes.

Reconciliations

.114 Daily Reconciliation: The total dollar value of each day's credit card receipts must be compared with and reconciled to the underlying transaction records of goods, licenses, etc., sold or issued.

a. Total credit card receipts from all systems must be reconciled to the total dollar value of the underlying transaction records (i.e., the number of products sold or licenses issued multiplied by applicable unit prices).

b. If the total credit card receipts do not agree to the total dollar value of the underlying transaction records, a transaction-by-transaction analysis must be performed to locate the difference.

c. Differences must be identified and corrected prior to clearing the deposit.

.115 Bank Reconciliation: The daily total for credit card receipts must be reconciled to the daily treasury statement received from OST, and the daily treasury statement must be reconciled to the Statewide Financial Management Application (SFMA**)** or the agency's cash management system.

Small volume transactions may be reconciled on a less frequent basis, such as weekly, but not less than once a month.

.116 Inventory Reconciliation: Settlement files must be reconciled with inventory records and/or customer databases on a regular basis.

Merchant Fees and Expense Recognition

.117 Merchant fees for all Visa and MasterCard transactions are deducted monthly from agencies' accounts at OST. Merchant fees associated with the Discover Card program are billed separately. Regardless of the method, agencies must review their US Bank Merchant Statements to ensure that the amounts charged for merchant fees are appropriate.

.118 For accounting purposes, merchant fees are recognized as an expense by recording them in comptroller object 4730. The related credit card revenue is recorded at the gross amount. For more information on expense recognition related to merchant fees, refer to **OAM 15.40.00.PO**, Expenses, Expenditures and Payables.

Refund Policy

.119 No cash refund shall be processed as the result of a credit card transaction including, but not limited to cash back requests, returned or undeliverable product, or an otherwise cancelled transaction.

a. The amount charged to the card must be fixed by the amount of the transaction.

b. Credits (refunds) must be issued to the same credit card used to process the original purchase transaction.

c. If the original credit card has been cancelled or has expired, a warrant or check refund may be issued upon receipt of a copy of the credit card reject document.

d. The agency's credit (refund) policy must be clearly displayed or otherwise communicated at the time of the initial transaction.

Chargebacks

.120 A chargeback is the reversal of the dollar value, in whole or in part, of a particular transaction by the card issuer to the state agency that originally processed the transaction. Chargebacks generally arise from customer disputes, fraud, processing errors, authorization issues and non-compliance with copy requests. It is recommended that agencies respond immediately to chargebacks and copy requests. Refer to the MTOS/MOR for further information and appropriate actions.

Segregation of Duties

.121 An adequate segregation of duties increases the likelihood that unintentional and intentional errors, including fraud, will be prevented or detected on a timely basis.

.122 Typical credit card functions that must be performed by separate individuals*, whenever possible*, include the following:

a. Processing the payment/authorization
b. Processing voids
c. Processing credits and refunds
   - Identifying credits

- Approving credits
- Issuing credits

d. Settlement
e. Handling billing and settlement errors
f. Reconciling

Credit Card Records Exempt from Public Disclosure

.123 All paperwork, records, receipts, card imprints, electronic data, etc., containing information provided to, obtained by or used by a public body to authorize, originate, receive or authenticate a transfer of funds, including but not limited to a credit card number, payment card expiration date, password, financial institution account number and financial institution routing number are exempt from disclosure under ORS 192.410 to 192.505 unless the public interest requires disclosure in the particular instance. **ORS 192.501(27) – Public Records Law**

Record Retention Requirements

.124 In general, copies of credit card receipts and supporting documentation must be retained by state agencies for 6 years (or in accordance with current archive requirements). However, copies of credit card receipts containing more information about a customer than the customer's name and five digits of the customer's card number must be destroyed on or before the sooner of:

a. The date the image of the copy is transferred onto microfilm or microfiche; or

b. Thirty-six (36) months after the date of the transaction that created the copy (**ORS 646A.204**).

Safeguarding Credit Card Records and Files

.125 Any agency that owns, maintains or otherwise possesses data that contains a consumer's personal information, including credit card information, must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including secure disposal of the data, in accordance with the Oregon Identity Theft Prevention Act (Oregon Laws 2007, Chapter 759).

.126 An agency shall be deemed to have met the requirements of the Oregon Identity Theft Prevention Act, if the agency is subject to and complies with:

a. Regulations promulgated pursuant to Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. 6801 to 6809), as the act existed on October 1, 2007.

b. Regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as the act existed on October 1, 2007.

.127 An agency shall also be deemed to be compliant with the Oregon Identity Theft Prevention Act, if it implements an information security program that includes these safeguards:

a. Administrative safeguards such as the following, in which the agency:

- Designates one or more employees to coordinate the security program;
- Identifies reasonably foreseeable internal and external risks;
- Assesses the sufficiency of safeguards in place to control the identified risks;
- Trains and manages employees in the security program practices and procedures;

- Selects service providers capable of maintaining appropriate safeguards and requires those safeguards by contract; and
- Modifies the security program in light of business changes or new circumstances.

b. Technical safeguards such as the following, in which the agency:

- Assesses risks in network and software design;
- Assesses risks in information processing, transmission and storage;
- Detects, prevents and responds to attacks or system failures; and
- Regularly tests and monitors the effectiveness of key controls, systems and procedures.

c. Physical safeguards such as the following, in which the agency:

- Assesses risks of information storage and disposal;
- Detects, prevents and responds to intrusions;
- Protects against unauthorized access to or use of personal information during or after the collection, transportation and destruction or disposal of the information; and
- Disposes of personal information after it is no longer needed for business purposes or as required by local, state or federal law by burning, pulverizing, shredding or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed. The agency may contract with another person engaged in the business of record destruction to dispose of personal information in a manner consistent with this paragraph.

.128 Any media (paper, electronic, or other) containing confidential cardholder information must be protected from unauthorized access and/or disclosure at all times. Backup media must likewise be securely stored. Paper documents containing confidential information must be stored in secure areas and/or in locking cabinets. Procedures to ensure the security of the keys or other locking mechanisms are also required.

.129 Networks or other devices, including point-of-sale terminals, used to store, process or transmit confidential credit card information collected from customers must be secure. Agencies must comply with the ISO/IEC 27002 Standard or the security architecture component of the Statewide Technical Architecture standard. ISO/IEC 27002 is an international information technology management standard that provides a generic set of best practices for use by those involved in initiating, implementing, or maintaining information security in an organization. The controls addressed by these standards include, but are not limited to, adequate physical and logical access security such as firewalls, data storage and transmission encryption, limited access to computer hardware, hardening servers, and regularly changed strong passwords.

Security Breach and Notification Requirements

.130 Under the Oregon Identity Theft Prevention Act, any agency that maintains personal information, including credit card information, of Oregon consumers must notify its customers if computer files containing that personal information have been subject to a security breach. The notification must be done as soon as possible, in one of the following ways:

a. Written notification.

b. Electronic, if this is the customary means of communication between an agency and its customers.

c. Telephone notice, provided that the agency can directly contact its customers.

.131 If an agency can demonstrate that the cost of notifying customers would exceed $250,000, that the number of those who need to be contacted is more than 350,000; or if the agency does not have the means to sufficiently contact consumers, the agency may give substitute notice. Substitute notice consists of:

a. Conspicuous posting of the notice or a link to the notice on the agency's website, if one is maintained, and

b. Notification to major statewide Oregon television and newspaper media.

.132 Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation.

.133 If an investigation into the breach or consultation with a federal, state or local law enforcement agency determines there is no reasonable likelihood of harm to consumers, or if the personal information was encrypted or made unreadable, notification is not required.

.134 If the security breach affects more than 1,000 consumers, the agency must report to all nationwide credit-reporting agencies the timing, distribution, and the content of the notice given to the affected consumers.

.135 Any state agency that is subject to and complies with the notification regulations or guidance adopted under Gramm-Leach-Bliley Act meets Oregon's requirements. However, if the breach involves the personal information of employees, the agency must follow Oregon's notification requirements.

.136 Agency resources, including best practices, checklists, sample notification letters and other tools, are available at the following websites:

a. Department of Consumer & Business Services: http://dfr.oregon.gov/Pages/index.aspx

b. Department of Administrative Services, Enterprise Information Strategy and Policy Division, Enterprise Security Office: http://www.oregon.gov/DAS/OSCIO/Pages/Security.aspx

Compliance with Payment Card Industry Standards

.137 Agencies that store, process or transmit cardholder information associated with credit card transactions must also comply with applicable industry data security standards. Visa, MasterCard, American Express, and Discover card brands require compliance with the Payment Card Industry Data Security Standard (PCI-DSS). The PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. **Failure to comply with industry standards may result in fines and/or revocation of credit card acceptance.**

.138 State agencies are required to implement a credit card processing system that does not store the following sensitive authentication data subsequent to authorization of the transaction:

a. The full contents of the magnetic stripe on the back side of the credit card.

b. The card validation code or value (the three-digit or four-digit number printed on either the front or back of the credit card).

c. The personal identification number (PIN) or the encrypted PIN block.

.139 The PCI-DSS also requires entities to develop internal policies and procedures that address credit card handling from the time information is received through its secure disposal. Examples of policy areas include:

a. Credit card processing procedures for agency staff and supervisors.

b. Access to credit card systems and information.

c. Security policy for credit card transactions.

d. Incident response plan for data breaches.

e. Storage of sensitive information, data retention and disposal policy.

.140 Agencies that accept credit cards as a payment option should work with OST to ensure they are PCI-DSS compliant and have successfully mitigated the risks associated with this payment option.

Third Party Service Organizations

.141 Third party service organizations that provide storage, processing, or transmission services and/or applications to state agencies associated with credit card transactions must be prequalified by the Office of the Treasurer (OST). Prequalification provides assurance that these vendors have met minimum industry and state security, interface, and depository requirements. In addition, OST will require an annual requalification to ensure that all approved vendors remain qualified. For more information on third party vendor requirements in connection with credit card transactions, refer to **OST Policy 02 18 14.PO**.

OREGON ACCOUNTING MANUAL

SUBJECT:	Internal Control	**Number:** 10.40.00
DIVISION:	Chief Financial Office	**Effective date**: June 1, 2012
Chapter:	Internal Control	
Part:	Expenditures	
Section:		
APPROVED:	George Naughton, Chief Financial Officer	Signature on file

PURPOSE: This policy sets **accountability** standards for **agency heads** and employees with delegated commitment and expenditure authority. It defines accountability for all employees within a given risk environment. Oregon statutes give agency heads the responsibility for approving the use of state resources for commitments, **expenditures**, and disbursements of their agency.

AUTHORITY:

ORS 98.352
ORS 291.015
ORS 291.990
ORS 293.275
ORS 293.295
ORS 293.306
ORS 293.330
ORS 293.375
ORS 293.450
ORS 293.455
ORS 293.460
ORS 293.475
ORS 293.480
ORS 293.485
ORS 293.490
ORS 293.495
ORS 293.590

APPLICABILITY: This policy applies to all state agencies included in the state's annual financial statements, except for those agencies specifically exempted by OAM Policy 01.05.00.

POLICY:

Employee Responsibility

101. An agency head is authorized to make expenditure decisions by statute and legislative appropriation. If the agency head delegates **expenditure decision authority** to subordinates, it must be in writing. Any person who exercises expenditure decision authority will be legally responsible and accountable for the expenditure. The agency head or approving officer can be held responsible or accountable for another's expenditure, especially when he or she knows the expenditure is unlawful or contrary to agency policy. The person exercising expenditure decision authority directs another person to make a purchase or incur an expenditure. The person following this direction will not be held responsible or accountable for the expenditure unless the person being directed clearly knows the expenditure is unlawful.

102. Each employee authorized to make an expenditure decision involving **state funds** is responsible for the "good judgment" and "lawfulness" of the expenditure. He or she must ensure that the transaction is for authorized purposes and is a responsible and appropriate use

of the funds. A negligent or fraudulent expenditure can result in personal financial responsibility and disciplinary action up to and including dismissal.

103. The following four criteria must be met for payment of a **claim** against money in the State Treasury:

    a. The agency that incurred the **obligation** or made the expenditure must possess an approval document signed by an **approving officer**.

    b. Provision for payment of the claim must be by law and appropriation.

    c. The obligation or expenditure on which the claim is based must be authorized by law.

    d. The claim otherwise satisfies requirements as provided by law.

104. The agency head should initiate and complete appropriate corrective action when subordinates violate policy. He or she should maintain appropriate documentation supporting delegated authority, approved payments, and corrective actions.

105. The controller or chief financial officer may assist the agency head in monitoring compliance with the agency's accountability policy. Periodic reviews of agency expenditures by the agency head help to assure appropriateness. Agency management should ensure that adequate internal management controls exist to give reasonable assurance of compliance.

Fiscal Office Responsibility

106. Accounting office personnel without delegated expenditure decision authority or any pre-audit responsibility are responsible for the accuracy of their actions in processing claims based upon the information available to them. Claim processors should exercise reasonable care in performing the duties assigned to them. Likewise, **employees who execute payment documents** do not have expenditure decision authority unless specifically designated.

Penalties for Inappropriate Action

107. Consideration of risk, materiality, and required effort are key elements in management's evaluation of necessary controls. While waste and abuse must be controlled and eliminated, the controls must serve a good business purpose and be cost beneficial.

108. Although unusual, there are occasional cases of employee dishonesty. Any suspected dishonesty case will be handled according to **ORS Chapter 278** and Department of Administrative Services Risk Management policy. Additional information is available on the Risk Management website at http://www.oregon.gov/DAS/Risk/pages/index.aspx .

109. Inappropriate actions by people authorized to expend state funds may result in penalties. In some cases, there could be denial of the state's insurance protection for employees when purchases were not for appropriate purposes. The following are typical consequences relating to different levels of inappropriate expenditures:

    a. A simple error is an unintentional action that was thought at the time to be proper but discovered later to be inappropriate. There is no penalty for a simple error as long as it is not part of a pattern of simple errors. Such a pattern may move the action to the negligence category.

b. Negligence is failure to act reasonably under existing circumstances. An employee may incur disciplinary action for expenditures that are negligent or contrary to state or agency policy.

c. Gross negligence is wanton or reckless disregard of one's duty of due care. The penalty for gross negligence may include personal financial responsibility and disciplinary action up to and including dismissal.

d. Fraud is intentional material misrepresentation or omission when there is a duty to disclose a loss or unlawful diversion of public funds. Theft is intentional diversion of state property to personal use. The penalties for fraud and theft may include personal liability; disciplinary action up to and including dismissal; and criminal sanctions.

110. In addition to the sanctions described in the preceding section, the state may refer instances of abuse that violate other statutes to the appropriate law enforcement authority. These referrals may include, but are not limited to, criminal prosecutions for theft (**ORS 164.015 - 164.125**) or abuse of public office (**ORS 162.415**) and proceedings for violations of the Oregon Ethics in Government Act (**ORS chapter 244**).

111. The Code of Ethics for state employees (**ORS 244.040**) provides that no employee can gain personally from his or her employment. Courts have declared that public office is a trust for the benefit of the public that the government serves. It is the duty of all public officers and employees to exercise good judgment and common sense in obligating and expending the resources of the state. Each employee must take responsibility for the wise use of state resources.

PROCEDURE:

Standard Payment Process

112. The State Treasurer pays on demand all sums authorized by law if there are appropriate and sufficient funds in the Treasury to make the payment; pays all warrants drawn on the Treasury in the order in which the warrants are presented out of the appropriate fund; and pays no amount out of the Treasury except when allowed by law.

Expenditure Authority, Responsibility, and Accountability

113. Each agency head must document the delegation of expenditure decision authority to specific individuals. He or she must ensure policies and procedures are in place and that they are consistent with this policy and describe the required documentation, the approval process, the penalty or correction process and criteria, and any delegated responsibility. Required documentation must be maintained for audit purposes. For agencies using electronic approvals, the delegation listing must be kept current to document the authorizations made. (Forms for establishing signature authority are available from the State Treasury at http://www.oregon.gov/treasury/Divisions/Finance/StateAgencies/Pages/Cash-Management-Forms.aspx .)

114. **Payment documents** used to authorize expenditures include invoices, entitlements, awards and grants, grant disbursement requests, vouchers, check requests, insurance claims, **purchase orders**, contract release orders, travel claims, personnel actions for payroll transactions, and other similar forms. When an approving officer with sufficient delegated authority approves these or similar documents, claim processors make the payment in a timely

way consistent with good cash management practices. Claim processors can rely on the approval as the only necessary authorization to make payment if so directed by agency policy.

115. Employees independent of the claims and payables process should review claim payments internally for accuracy and appropriateness.

Evaluation of Commitment or Obligation

116. Careful review of any expenditure, encumbrance, or obligation by the approving officer includes asking appropriate questions. These evaluations are not required of the controller or chief accounting officer unless so delegated by the agency head. The following questions are examples and are not all-inclusive. They are recommended for approving officers because of their potential liability.

    a. Is this a legal obligation for the state to incur? Does it comply with statute and policy?

    b. Is this obligation a responsible and appropriate use of these funds for this agency and for the state as a whole?

    c. Did the agency receive the goods or services at full value as requested?

    d. Are there adequate budget resources available now to allow us to incur this obligation?

    e. Will this obligation or expenditure pass the "public perception" test? That is, would I be comfortable if I saw this transaction written up on the front page of the local newspaper?

    f. Am I willing to approve this obligation knowing that I am fully responsible?

Authorization of Obligation

117. Contracts, purchases, invoices, grants and expenditure claims are approved by an approving officer who authorizes the state obligation. If in doubt about the appropriateness of an expenditure, the approving officer could consider documenting his or her rationale and the reasonable business purpose of the expenditure.

118. The signature or electronic approval of the approving officer means that adequate funds are available with existing budgetary authority, that this is an appropriate and authorized expenditure of state resources, that personal financial liability could be assessed if later determined to be an inappropriate expenditure of state funds, and the person authorizing the expenditure is authorized to make it. The following are specific meanings for certain approvals:

    a. State Purchase Order or Contract Release Order. Approval means the items purchased are authorized by or comply with the Department of Administrative Services' policies and procedures and that provision for payment is by law and appropriation to cover this purchase. In addition, approval means this purchase is allowed by statute and is a responsible and appropriate use of these funds.

    b. Invoices and credit card charges. Approval means the materials, services, or other expenses covered by the claim have been furnished, rendered, or expended on behalf of the state. Approval means the provision for payment is by law and appropriation, the obligation or expenditure is authorized by law, and the claim satisfies the requirements as provided by section 103 above. The claim has been approved for payment in a specific amount.

c. Travel Claims. After the traveler certifies the accuracy and appropriateness of the claim, the approving officer should approve the claim. A commissioner, board member, or other approving authority in an agency will approve the agency head's travel claims. The approval signature means that expenses claimed are valid and authorized "duty required" expenses, the expenses comply with current travel policies and **ORS 292.220**, and that provision for payment is by law and appropriation.

d. Payroll Actions and Personnel Action Forms. Approval means the person named on the form is an employee of the state in a permanent or temporary position authorized by the legislatively approved budget, that provision for payment is by law and appropriation to pay the salary and benefits indicated, and that the approval signature is that of the designated appointing authority.

e. Entitlements, Awards, and Grants. Approval means that the "grantee" meets the criteria for the award, that provision for payment of the award is by law and appropriation, and that the current disbursement complies with the provisions of the grant or contract and any related federal requirements.

f. Other Claims. Approval means the expenditure is legally authorized and is a responsible and appropriate use of the funds, provision for payment is by law and appropriation, and the approval is by an authorized employee of the state.

119. Documentation must show that an agency has received proper value, as defined by agency management, and has complied with **ORS 293.295** before a voucher is authorized for payment. This may consist of evidence that (a) goods or services have been received; (b) items delivered were as specified; (c) prices, terms, and extensions shown on the vendor's invoices are correct. Agencies should pay vouchers by the due dates to take advantage of maximum discounts.

120. An optimum standard of control over the processing of payments for purchases of goods or services, benefit or similar payments, and refunds would provide a three-way match of documents. The match may include the following with each item originating from a separate, unrelated work unit.

a. The authorization or payment request is sent to the disbursement unit.

b. Receipt of goods or services or eligibility for payment is sent to the disbursement unit.

c. Incoming invoices, if applicable, are delivered directly to the disbursement unit.

d. The disbursement unit proofs invoice amounts, matches all related documents, and prepares a voucher or check for the appropriate payment.

121. The state pays overdue account charges incurred by state agencies that do not promptly pay for goods and services provided by private businesses. Claims are considered "overdue" if a check or warrant is 45 days from the date the agency received the invoice, or the date of the initial billing statement if no invoice is received, or the date the claim is certain by agreement of the parties or by operation of law. Overdue account charges will not exceed 8-percent per annum and are to be paid against an agency's appropriation or limitation.

Expiration of Warrants and Checks

122. All warrants and checks issued by state agencies will include in at least 8-point type this statement, "VOID AFTER 2 YEARS FROM DATE OF ISSUE." Checks and warrants that are

computer-generated may use a computer printed statement; all other checks will require the statement to be typed or stamped.

123. Annually between October 1 and November 1, SFMS Operations will prepare a list of all unpaid warrants issued for a period of more than two years prior to July 1 of the year the list is prepared. Agencies due diligence responsibilities include making at least one attempt to find the vendor no later than 90 days prior to October 1 for all warrants $100 or more. Agencies may not charge the vendor for the search and must keep records of their attempt for three years. All warrants appearing on the list will be expired in R*STARS.

124. Annually, between October 1 and November 1, each agency that maintains a checking account will prepare from its records, and certify to the Department of State Lands, a list of all checks that are outstanding and not paid by the State Treasurer for a period of more than two years prior to July 1 of the year the list is prepared.

125. After October 1 of each year, the State Treasurer may refuse payment of the outstanding checks on the lists of checks and warrants more than two years old. Statewide Financial Management Services (SFMS) staff will debit general fund cash and credit deposit liability for the amount of the expired General Fund warrants. SFMS will instruct transfer of all other amounts related to unpresented warrants to the Department of State Lands for deposit in the Unclaimed Property Revolving Fund within the Common School Fund Account. Agencies will instruct transfer of all other amounts related to unpresented checks to the Department of State Lands. The lawful owner of any check or warrant expired after two years may file a claim with the Department of State Lands. If the Department of State Lands is satisfied that an unpaid check or warrant is for a valid claim, the state will pay the check or warrant and charge the originating fund.

Duplicate Instruments

126. No warrant or check will be paid until such warrant or check, or duplicate thereof, is surrendered to the State Treasurer. A duplicate warrant or check may be issued if the lawful owner furnishes a notarized affidavit that satisfies the payment officer that the original instrument was lost, stolen, or destroyed. Any agency that receives a request to issue a duplicate Department of Administrative Services warrant should send a request for Stop Payment of the original warrant to SFMS Operations. Once the agency has received a notarized affidavit from the lawful owner, the agency may issue a replacement warrant to the claimant.

127. The issuing agency must search for the original instrument out of the paid instruments returned to the agency from the State Treasurer. Copies of truncated R*STARS redeemed warrants may be obtained by contacting the Cash Management Section of the State Treasury. Refer to http://www.oregon.gov/treasury/Divisions/Finance/StateAgencies/Pages/Cash-Management-Forms.aspx. If the original instrument is found, a copy of both sides will be furnished to the person applying for a duplicate instrument. If the applicant determines beyond any doubt that the endorsement is a forgery, he or she must submit an affidavit of forgery. The agency returns the original instrument or authentic reproduction immediately to the State Treasurer who will promptly return the instrument to the presenting or payor bank for credit. The State Treasurer will not be liable for his or her inability to obtain credit from the presenting or payor bank for an instrument returned without credit.

128. Each agency that lawfully issues checks upon the State Treasurer must have a procedure of issuing duplicate instruments. Agencies may adopt the uniform procedure of issuing and delivering duplicate instruments to people entitled to replacement of lost, stolen, or destroyed instruments.

129. If an instrument is paid in an unauthorized manner, the wrongful payment will not relieve the agency issuing the instrument from liability to the true and lawful owner. The person making the wrongful payment and the sureties on his or her official bond, if any, must pay the full amount of the loss.

Death of Payee

130. If the payee of a warrant or check drawn on the State Treasurer dies after issuance of the instrument without receiving payment and the payee's estate is not probated, the authorized survivor(s) of the payee may obtain payment after completing the following two actions:

a. Surrender the instrument to the State Treasurer with endorsement in the name of the payee and of herself or himself, or themselves as survivor(s); and

b. File with the instrument an affidavit to the effect that the affiant(s) is (are) the survivor(s) of the person entitled to the proceeds of the instrument.

Payment will be made to the survivors as prescribed by **ORS 293.490** and **293.495**.

OREGON ACCOUNTING MANUAL		Number 10.40.10
Oregon Department of Administrative Services State Controller's Division	**Policy**	Effective Date July 28, 2003
Chapter	**Internal Control**	.1 OF .4
Part	**Expenditures**	
Section	**Non-travel Meals and Refreshments**	Approval Signature on file at SCD

Authority **ORS 291.015**
ORS 293.295
ORS 293.330
ORS 293.590

Purpose and Applicability

.101 This policy provides guidelines to **agencies** concerning when meals and refreshments may be paid for with **State funds**. Applicability of this policy is limited to non-travel business meals and refreshments. *Non-travel business* would include meetings, training sessions, conferences, or other agency-sponsored events to conduct official state business. This policy does not apply to reimbursement (through submission of travel expense claim) or provision (provided by agency directly) of meals and refreshments to employees or authorized non-state individuals, including volunteers and board or commission members, while the employee or individual is on travel status. See **OAM 40.10.00** (travel policy) for situations in which the employee or authorized non-state individual, including volunteer, is on travel status.

.102 As noted in **OAM 10.40.00**, Internal Control – Expenditures, employees authorized to obligate State funds are responsible to ensure the expenditure is appropriate and lawful. Public employees may be personally liable for obligations that are inappropriate or an improper use of State funds. As with any expenditure, **agency heads** and employees with delegated **expenditure decision authority** are responsible to determine the appropriateness of purchases and to ensure that sufficient documentation exists to support the expenditure. The purchase must serve the business needs of the agency, and authorization must be provided prior to obligation of funds. This policy is intended to provide guidelines to help decision-makers determine the prudence of purchasing non-travel meals and refreshments with State funds. The cost of non-travel meals and refreshments should be reasonable and not excessive.

.103 Agency management is responsible for establishing procedures to implement this policy. Individual agencies may adopt policies on meals and refreshments that are more restrictive than this policy, at the discretion of the agency.

Meals

.104 Meals are defined to include food and beverages provided at breakfast, lunch, or dinner to attendees of agency-sponsored functions.

.105 State funds must not be used to provide non-travel business meals for regularly scheduled staff meetings. In addition, state funds must not be used to provide non-travel business meals for business meetings where the majority of participants are state employees, except as allowed in (a), (b), and (c) below:

a. Even when the majority of participants are state employees, a non-travel business meal may be provided at legal proceedings such as a hearing, trial, deposition, or mediation. At the discretion of the agency, a meal may be provided when an employee is participating in legal proceedings and the meal is served during the course of the proceedings or the cost of the meal is incurred as a part of preparing a participant for ongoing legal proceedings.

b. Even when the majority of participants are state employees, a non-travel business meal may be provided at training sessions and conferences attended by a minimum of 25 participants. For training sessions and conferences attended by less than 25 participants, agencies should apply professional judgment to consider whether participants can reasonably be expected to obtain and consume a meal on their own based on proximity to available food service and return within an hour. If participants cannot reasonably be expected to obtain and consume a meal on their own based on proximity to available food service and return within an hour, a meal may be provided with State funds. When a meal is provided at training sessions and conferences, it is not necessary that business be conducted during the meal period.

c. Even when the majority of participants are state employees, a non-travel business meal may be provided to participants of board and commission meetings (boards and commissions must be approved by statute) when a business meeting is held over a normally scheduled meal period and the meeting is at least 3 hours long. Participants may include staff, but only those essential for the conduct of business.

.106 In addition to .105 above, State funds must not be used to provide non-travel business meals for employees or other participants, except as noted in paragraph .107 below.

.107 A meal may be provided to attendees when a business meeting includes a working business meal at which the attendance of participants is required, and the meal period is designated as a work session, which is documented in the meeting agenda. Business must be conducted during the meal period and a benefit to the State must be gained by providing the meal as part of the agenda rather than dismissing attendees to obtain a meal. For example, benefits may be gained in that providing a meal maintains continuity, promotes safety, or enables resumption of duties.

Refreshments

.108 Refreshments are defined to include beverages such as coffee, tea, bottled water, juice, soda, and similar liquid refreshments as well as sugar and creamer. Food items such as fruit, pastries, chips, cookies, cake, candy, etc., are also considered refreshments.

.109 State funds must not be used to provide refreshments for:

a. Regularly scheduled staff meetings.

b. Office social events such as celebrating holidays or birthdays.

c. Voluntary social events (either off-site or in the office) such as agency-sponsored retirement celebrations.

.110 State funds may not be used to purchase bottled water and/or water dispensers for offices, except when water has been officially tested and found to be unsafe for drinking purposes, or in cases of permanent or temporary water unavailability. In temporary situations, agencies should document the circumstances as justification for the need to purchase water.

.111 State funds may only be used to purchase alcoholic beverages if an agency has an appropriate business-related function. In addition, agencies that purchase alcoholic beverages for business-related functions must comply with Risk Management Policy 125-7-401 (see http://www.oregon.gov/das/Risk/Pages/Insself.aspx.

.112 Alcoholic beverages in paragraph .111 above do not include alcoholic beverage products purchased for commercial distribution, such as operations of the Oregon Liquor Control Commission.

.113 At the discretion of the agency, State funds may be used to provide refreshments for the purposes or events listed below.

a. Business meetings with industry representatives or the public. This may include events such as task force, advisory board, or commission meetings.

b. Business meetings involving state employees that are scheduled to last 4 hours or longer and cafeteria services are not reasonably available.

c. Business meetings or training events when the majority of personnel attending are called in from field office locations outside the city where the meeting or training is taking place.

d. Training events held for the purpose of instruction or dissemination of information to state employees and/or the general public.

e. Staff retreats held for the purpose of the agency's work-related planning.

f. Agency-sponsored employee recognition or volunteer recognition programs.

g. When refreshments are included as a non-separable portion of the cost of renting a facility.

h. As a gesture of appreciation to volunteers during or after work is performed.

Related Items

.114 Essential serving products such as paper plates, cups, and plastic utensils may be purchased with State funds, as long as the purpose or event meets the guidelines for purchasing meals or refreshments outlined in this policy.

.115 Other related items such as those listed below may not be purchased with State funds:

- Holiday decorations
- Indoor house plants or flower arrangements
- Retirement invitations, cards, gifts, and party favors
- Punch bowl sets or other specialty serving containers

.116 Related items in paragraph .115 above do not include serving containers or other items used in commercial operations such as conference rental facilities operated by state agencies or promotional items that support an agency's business mission.

Documentation and Payment

.117 When meals or refreshments are provided for a given event, the following record keeping should be used to account for the use of State funds:

a. Written agenda for the meeting documenting that it was a working business meal. For training sessions and conferences, there is no requirement that business be conducted during the meal; however, a written agenda of the training session or conference is required.

b. Written list of meeting attendees, including the number of state employees versus the number of non-state employees (in cases where personal identity is confidential or sensitive in nature, a number of attendees is sufficient; however, the number of state employees versus the number of non-state employees should still be indicated).

c. An itemized invoice or receipt, including unit costs, from the vendor who provided the meals and refreshments.

.118 The written agenda and list of attendees (or number of participants) should be attached to the invoice for payment to vendors for meals and refreshments.

.119 If a questionable or inappropriate payment is made that does not comply with the guidelines outlined in this policy, agency management should take appropriate action, including obtaining reimbursement from the employee who authorized the purchase.

OREGON ACCOUNTING MANUAL		Number 10.50.00.PO
Oregon Department of Administrative Services State Controller's Division	**Policy**	Effective Date July 1, 2001
Chapter	**Internal Control**	.1 OF .2
Part	**Capital and Non-capital Assets**	
Section		Approval Signature on file at SCD

Authority **ORS 270.010**
ORS 276.227
ORS 278.005
ORS 278.011
ORS 278.405

Real Property

.101 It shall be the policy of the State to hold in State ownership no more **real property** than is necessary to conduct official business, with allowance for reasonably foreseeable demands of the future. The acquisition, sale, exchange, lease, retention, and management of State-owned real property shall be subject to a statewide plan. The plan will encourage the transfer through sale or lease of property already in State ownership to private ownership and use. The plan's objective will be to minimize State investment in such land and place such land on the tax rolls.

.102 The State recognizes that providing and operating State government facilities is a significant capital investment. Accordingly, it is the policy of the State to plan, finance, acquire, construct, manage, and maintain its facilities in a manner that maximizes and protects this investment.

Personal Property

.103 Agency management is responsible to ensure that internal controls are sufficient to provide reasonable assurance that State assets are not lost or stolen.

.104 The administrative head of each agency has a responsibility to maintain a system (manual or automated) which will assure that the State's property (**capital** and **non-capital**) is accounted for and classified properly, accurately, and systematically. The agency administrator will appoint an individual to maintain this system. Refer to the OAM 15.60.00 Chapters for guidance on accounting for capital assets or **OAM 15.55.00** for non-capital assets.

.105 Functional responsibilities for capital assets that agencies should delegate to separate departments or management levels are:

- Planning and approval of capital expenditures.
- Authority to idle, sell, or otherwise take assets out of production.
- Data processing of capital asset acquisition and payment transactions.
- Physical custody and operating responsibility for use of assets.
- Reconciliation of the inspection (inventory) of capital assets to the subsidiary records.

Insurance

.106 The State pays, through the Insurance Fund, its cost of restoring most State property that may be lost, damaged or destroyed. The purpose of self-insuring is to restore property needed for the operations of the State. The Insurance Fund is meant to reimburse for accidental loss, not to substitute for the duty of each agency to prevent and reduce loss or to maintain good repair.

.107 For officer, employee, and **agent** dishonesty losses covered by Risk Management Policy, the State is self-insured. One deductible applies to each loss as follows:

a. Five thousand dollar ($5,000) deductible for employee dishonesty. If an agency had a loss control or fiscal management program in place prior to the loss which, if followed, would have minimized the loss, Risk Management will reduce the deductible to $500.

b. Two hundred fifty thousand dollar ($250,000) deductible for unfaithful performance (employee's failure to perform certain duties prescribed by law). This may change without notice.

OREGON ACCOUNTING MANUAL		Number 10.50.00.PR
Oregon Department of Administrative Services State Controller's Division	**Procedure**	Effective Date January 2, 2002
Chapter	**Internal Control**	.1 OF .5
Part	**Capital and Non-capital Assets**	
Section		Approval Signature on file at SCD

Authority
ORS 270.020
ORS 270.100
ORS 270.180
ORS 276.180
ORS 276.227
ORS 278.405
ORS 283.337
ORS 283.343
ORS 283.350
ORS 293.590

.101 **Capital assets** are all tangible or intangible property used in an agency's operations that have initial estimated useful lives beyond a single year and have an initial cost (inclusive of **ancillary charges** necessary to place the asset into its intended location and condition for use) of at least $5,000. Items below the $5,000 threshold should not be capitalized. Examples of capital assets include land, land improvements, buildings and building improvements, motor vehicles, equipment and machinery, works of art and historical treasures, and **infrastructure** items such as state highways and airports**.**

.102 **Non-capital assets** are all tangible and intangible property used in agency operations that have initial estimated useful lives beyond a single year and have an initial cost (inclusive of ancillary charges) of less than $5,000. Although non-capital assets should not be capitalized, agency management should determine which of these assets is at high risk of loss (e.g. laptop computers, firearms, hand tools, etc.) and should inventory and track these assets on a separate inventory listing. Public stewardship, risk, and internal control concerns should govern the agency's decision on how these assets are managed and tracked.

.103 Capital assets may be acquired by outright purchase, construction, lease purchase agreement, installment purchase contract, eminent domain, foreclosure, transfer from another fund or agency, or gift. Capital assets should be separated and recorded under the proper definition as land, land improvements, buildings and building improvements, equipment and machinery, data processing hardware, data processing software, works of art and historical treasures, and infrastructure.

.104 Reconciliations of capital outlay expenditures to capital assets should be completed by each agency on at least a quarterly basis.

Real Property

.105 DAS Facilities Division shall maintain and keep current an inventory of all State-owned property and shall classify all such property on the basis of current use, value, idle or surplus to the agency need. DAS shall establish categories of real property necessary for management of state-owned real property. Land owning agencies shall provide status information, as requested by DAS, of agency-owned land.

.106 When vacated and no longer required for institution uses, all or any portion of the buildings, grounds, and facilities presently operated and controlled by the Mental Health and Developmental Disability Services Division, Department of Corrections, State Office for Services to Children and Families, or the State Board of Education, are transferred to the DAS, if the Department of Administrative Services orders such transfer.

.107 Agencies are required to secure approval from DAS for sale of all other real property prior to disposition. Excepted agencies (Department of Fish and Wildlife, Department of Forestry, Department of Transportation, Division of State Lands, Oregon University System, Parks and Recreation Department) and agencies of the legislative or judicial branches must receive prior approval if disposition is for less than the fair market value of the land. A copy of the approval will be kept in the agency's control file.

.108 Property is removed from the property ledger only when title is transferred to another.

Vehicles

.109 DAS shall control and regulate the acquisition, use, maintenance, and disposal of motor vehicles used for State business.

.110 Agencies wanting to acquire passenger vehicles not listed on State price agreement shall seek and receive specific approval from the Joint Legislative Committee on Ways and Means or the Legislative Emergency Board before proceeding with vehicle acquisition through DAS purchasing.

.111 Exceptions to .110 above require signature approval of the administrator of the TPPS Division of DAS and shall be permitted in instances enumerated in DAS Fleet Policy. (See http://www.oregon.gov/DAS/EAM/FPS/pages/policies.aspx.)

.112 State vehicles deemed to have reached the end of their efficient life cycle shall be disposed of according to State law. Vehicles scheduled for disposal will be sold through DAS TPPS Division Surplus Property.

.113 State-owned sedans and station wagons must meet a minimum monthly mileage requirment. Vehicles not achieving the monthly mileage threshold as averaged over a designated six-month period may be subject to sale. Refer to DAS Fleet Policy http://www.oregon.gov/DAS/EAM/FPS/pages/policies.aspx.

.114 Agencies are responsible for obtaining the most cost-effective means of transportation for their employees. The most cost-effective alternative is motor pool vehicles. If a motor pool vehicle is not available, agencies may reimburse private car mileage, or approve rental of a vehicle through State price agreement. These choices should only be temporary until a Motor Pool vehicle is available.

.115 With few exceptions, the State's vehicles shall be stored at sites owned, leased, or controlled by the State. When practical, a State vehicle at home, hotel, or motel shall be parked off the street in a reasonably secure setting.

.116 An agency may allow a State vehicle to be parked at an employee's home when a task or trip requires the driver to depart so early or return so late that it is impractical to pick up or return the

vehicle to State Parking the same day. The agency must do a cost-benefit analysis before a long-term assignment of a vehicle to an employee's home.

.117 State owned or operated automobiles or trucks shall be marked, in plain lettering of readable size, with the name of the owning or operating agency, followed by the words "State of Oregon." Subject to the approval of the TPPS Division Administrator, vehicles owned or operated by State agencies may be unmarked when used by State agencies for specific purposes such as undercover criminal investigation.

.118 Agency management shall be responsible for acquiring vehicle services and replacement parts at the lowest possible cost and/or value to the State. Management shall also ensure that purchases and record keeping comply with State laws and generally accepted accounting principles.

.119 Custody of assets should be separated from recordkeeping. For instance, vehicle titles should be controlled by an individual in a unit separate from fleet storage and maintenance.

Inventory

.120 Personal property meeting the definition of capital assets should be capitalized, tagged with a State of Oregon identification tag and property control number, listed on the capital asset property inventory, and physically inventoried at least annually. Discrepancies should be investigated. Support that a physical inventory has been taken, for all locations, should be retained in the agency's central accounting office.

.121 As an individual agency policy, a lower level (below $5,000) may be used for inventory control purposes only (not for capitalization).

.122 Agencies should identify, record, and control inventory items that have a high risk of loss such as:

Computer and electronic equipment

Photography equipment

Firearms

Hand tools

Any other items agency management identifies as being at high risk of loss

.123 The agency should establish a separate listing for high risk and other assets below the $5,000 capitalization threshold that are inventoried. The separate listings can be inventoried concurrently or on a different frequency than the capital asset inventory. High risk assets that are assigned to state employees are subject to **OAM 10.55.00**.

Vehicle Records

.124 Agencies shall maintain records on each vehicle under their control. Records shall include:

a. Accurate vehicle inventory.

b. Reliable detailed and accurate information on work performed, replacement parts, and associated costs.

.125 Vehicle maintenance and repair records must accompany vehicles when transferred to another owner.

.126 Agencies shall maintain records and provide DAS with information necessary to comply with biennial legislative reporting requirements identified in ORS 283.343, Compliance Examination On Use Of State Owned Vehicles.

.127 Agencies shall maintain records and provide DAS with information necessary for the annual reporting requirements identified in ORS 283.337, Reports to Department of Environmental Quality and Office of Energy.

Insurance

.128 Each agency is required to file a Risk Report annually with the Risk Management Division of the Department of Administrative Services (DAS). Agencies are required to report all property in their possession on July 1 of each year on which the risk management policy would pay losses. Loss to property omitted from the report will not be paid. Loss to property acquired after report preparation will be paid subject to Risk Management policy. Refer to http://oregon.gov/DAS/EGS/Risk/Pages/PolicyHandbook.aspx.

.129 Conditions of coverage for employee dishonesty are:

a. Agencies must immediately report any and all losses discovered from apparent fraudulent or dishonest acts by agency officers, employees, or agents to the Risk Management Division and the Secretary of State Audits Division.

b. Agencies must report any and all losses within 90 days after they are discovered. Late reporting may forfeit coverage.

c. Agencies may not forgive, release, or promise not to prosecute any staff alleged to have caused a loss.

d. Agencies must preserve and furnish to Risk Management and the Audits Division all evidence of loss and of fraud or dishonesty.

Failure to comply with the above conditions may expose a state officer, employee, or agent to personal liability.

Disposition

.130 All personal property (including both capital and non-capital assets), when removed from the property ledger for ***any*** reason, must be removed by completion of the form designated by the DAS-State Surplus Property Program.

.134 Agencies should respond to directions from State Surplus Property Program for disposal of the surplus property. Do not delete property sent to surplus from the property control ledger until notified that the property has been sold or disposed of.

OREGON ACCOUNTING MANUAL		Number 10.55.00
Oregon Department of Administrative Services State Controller's Division	**Policy**	Effective Date February 1, 2002
Chapter **Internal Control**		.1 OF .1
Part **Employee Assigned Property**		
Section		Approval Signature on file at SCD

Authority **ORS 293.590**

Purpose

.101 This policy provides guidance for maintaining records of State property assigned to state employees, contractors, or volunteers.

Policy Standards

.102 Agency management is responsible for establishing procedures to issue and inventory property assigned to employees. State-owned property that may be assigned to state employees includes but is not limited to:

- Cell phones
- Pagers
- Palm pilots
- Keys and key cards
- Hand tools
- Laptop computers
- Cameras, camcorders, and photography equipment
- Televisions and VCRs
- Firearms
- Credit cards

.103 Records of property assigned to employees should be updated annually. The record should be used to document and assure that all property is returned to the State upon employee termination.

.104 Agencies that assign state-owned property to contractors should assure that the procedures for assigning and monitoring the use of the property are included in the contract. If state-owned property is assigned to volunteer workers, there should be a written agreement specifying how and when the property will be inventoried and how it should be returned upon completion of the volunteer assignment.

.105 Agencies should maintain an inventory of all property assigned to state employees, contractors, and volunteers and should make such inventory available for audit.

OREGON ACCOUNTING MANUAL

SUBJECT:	Accounting and Financial Reporting	**Number:**	10.60.00.PO
DIVISION:	State Controller's Division	**Effective date:**	August 1, 2010
Chapter:	Internal Control		
Part:	Information Technology		
APPROVED:	John Radford, State Controller		Signature on file at SCD

Authority **ORS 291.015**
ORS 293.590
ORS 293.595

Management of Risks, Performance, and Controls in the Information Technology (IT) Environment

.101 Each **agency head** is responsible for establishing, maintaining, and improving internal controls over the agency's information technology (IT). An agency must ensure the adequacy of the design, implementation, and operation of its IT controls to provide an acceptable level of confidence in agency systems and assurance that:

a. Management's IT goals and objectives are being accomplished effectively and efficiently;
b. IT investments and investment strategies are well planned and adequately funded;
c. IT assets are safeguarded; and
d. IT operational and investment strategies follow management's direction, authorization, and security and control policies.

.102 In addition, agencies must comply with all statewide IT security policies and initiatives issued by the Department of Administrative Services, Enterprise Information Strategy and Policy Division (DAS-EISPD) and all applicable federal and state laws and regulations pertaining to the confidentiality, integrity and availability of electronic data, including Oregon Laws 2007, Chapter 759.

.103 State agencies must provide adequate security and control training and other educational support to employees involved in the design, development, implementation, maintenance, and management of the IT infrastructure/function, as well as the storage and protection of the underlying data. A variety of nationally and locally recognized associations and DAS-EISPD provide training.

Review of IT Controls

.104 Periodically, agency management must review and test the performance of the agency's internal controls over information technologies.

.105 Agency management must prepare a report that identifies any significant or material weaknesses in the agency's IT controls and gives a status update on IT control weaknesses identified in earlier reports or noted by internal or external auditors. This report should be available for use by the

Department of Administrative Services as well as internal and external auditors. The agency must create a detailed plan for correcting the deficiencies and include estimated dates of completion.

.106 Agency heads should consider making the IT review process an annual event. The corresponding report would serve to document, as a permanent record, the effective management and control of the agency's IT operations and infrastructure investments.

.107 The Secretary of State, Audits Division has adopted CobiT (Control Objectives for Information and Related Technology) as the basis for auditing the IT management function. Agencies are also encouraged to adopt generally accepted standards relating to the IT management function.

.108 The Audits Division may review an agency's IT security and internal control management as part of its ongoing audit activities. Such a review will not satisfy the requirements of this policy for agency management to review and be accountable for the adequacy of the design, implementation, and operation of the agency's IT controls. However, suggestions from the Audits Division can be useful to agency managers in conducting IT reviews and formulating corrective action plans.

.109 The use of qualified agency internal auditors to assist management in reviewing IT controls is strongly encouraged. A properly staffed internal audit function may be able to provide ongoing monitoring and objective risk assessment. Independent review and analysis are critical elements in a well-designed framework of IT controls, particularly, during the planning, development, testing and implementation of systems.

OREGON ACCOUNTING MANUAL

Subject:	Accounting and Financial Reporting	Number:	10.60.00.PR
Division:	State Controller's Division	Effective date:	October 1, 2007
Chapter:	**Internal Control**		
Part:	**Information Technology**		
Section:			
Approved:	John Radford, State Controller	Signature on file at SCD	

Categories of Information Technology (IT) Controls

.101 In a computerized environment, controls are divided into two principal categories: general controls and application controls.

a. General controls are broad-based, pervasive controls that address the overall operation and activities of the information technology function. General controls apply to all information systems including mainframe, minicomputer, network, and end-user environments. They impact the entire data processing environment, including application systems. General controls address data center and network operations; system software acquisition and maintenance; physical security, environmental protection, disaster recovery, hardware maintenance and computer operations. Other examples include program change controls; controls that restrict access to programs or data; controls over implementation of packaged software or development of new software applications; and controls over system software that monitors the use of system utilities that could change financial data without leaving an audit trail.

b. Application controls, on the other hand, are more specific to individual application systems. They include both computerized and manual controls and are designed to help ensure the completeness, accuracy, and validity of all information processed. When data is transmitted from another system via an interface, application controls must be installed to ensure that all inputs are received and are valid and that all outputs are correct and properly distributed.

Segregation of Duties

.102 A primary aspect of general control includes the organization and operation controls related to the structure of the IT function and how duties are segregated. The IT organization is a support function in that it does not initiate or authorize transactions.

.103 In a well-structured IT organization, the following duties are segregated:

a. *Systems analysts* design the overall computer system. They decide what type of computer network is needed to accomplish management's goals and recommend changes to the overall network. The duties of the systems analyst must be segregated from the duties of the computer programmer and the computer operator.

b. *Application programmers* are responsible for writing the programs. The application programmer also handles the testing of programs, modification of existing programs, and preparation of computer operator instructions. The duties of the application programmer must be segregated from the duties of the systems analyst and computer operator.

c. *Systems programmers* are responsible for maintaining the operating system and related hardware. The systems programmer must not have access to application specific information about programs or data files. The duties of the systems programmer must also be segregated from the duties of systems analyst and computer operator.

d. The *computer operator* is responsible for maintaining live programs and data, scheduling processing activities, running programs, and distributing reports. It is critical that the computer operator and computer programmers be segregated; a person performing both functions would have the opportunity to make unauthorized and undetected program changes.

e. The *control clerk* logs and/or schedules the input and output as well as maintains the error and correction log. The clerk also controls the flow of batches through data entry and editing, monitors processing, and controls distribution of reports and other output.

f. The *IT supervisor* manages the functions and responsibilities of the IT organization and is a member of the external control group defined below.

g. The *external control group* usually consists of the data processing manager and other managers from user organizations. The external control group reviews input procedures; monitors data processing; reviews, approves and handles all reprocessing of errors; and verifies the proper distribution of data output.

h. The *file librarian* stores and protects the files, programs, and tapes from damage and unauthorized use.

i. The *security officer* is responsible for the assignment, maintenance, and timely changing of passwords. Passwords must never be written on paper and left in the workplace. The term *security officer* as used in this procedure refers to the role of the IT organization in controlling general systems access. This term is not synonymous with the term *agency security officer* as used in **OAM 10.70.00**; the agency security officer is responsible for authorizing and requesting access to the following financial systems or databases:

R*STARS (Relational Statewide Accounting and Reporting System)
ADPICS (Advanced Purchasing and Inventory Control System)
OSPA (Oregon Statewide Payroll Application)
Accounting Datamart (R*STARS reporting database)
Payroll Datamart (OSPA reporting database)

j. *System administrators* are responsible for keeping information up-to-date and restricting access. Database administrators update databases and limit access to appropriate personnel. Similarly, network administrators oversee the computer network, while web administrators manage information on the website. Duties of system administrators should, when possible, be segregated from programming and operation duties.

k. *Data input* personnel prepare, verify, and input data to be processed.

Systems Development Controls

.104 Systems development deals with the implementation of new systems and the modification of existing systems. Agency heads and chief information officers (CIOs) must assure all system, implementations, enhancements, and program modifications are appropriately authorized and documented.

.105 Agency heads and CIOs must submit a request identifying the need and outlining the steps to be taken for implementing new IT systems or modifying existing IT systems. Necessary elements include:

a. Proper approval by the State Controller's Division (SCD) and Enterprise Information Strategy and Policy Division (EISPD) to acquire or modify fiscal systems. Refer to **OAM 10.65.00.PO**, *Approval of Proposed Fiscal Systems*, and EISPD statewide policies concerning systems development.

b. Appropriate documentation describing the nature and logic of the proposed changes;

c. A proper methodology for testing and debugging all changes on a test system before incorporating the changes into an operable system;

d. A log of all system enhancements and modifications.

.106 No changes shall be made to programs and files until authorization is provided in writing, and only computer programmers are allowed to make the changes. The same control procedures that apply to the installation or modification of application programs also apply to changes in systems software (e.g., the operating system).

Documentation Controls

.107 There are three levels of documentation that must be maintained. Documentation at each level normally consists of flowcharts and a narrative description.

a. System documentation provides an overview of the programs and data files, how processing occurs, and how different programs within the system interact with each other. In essence, system documentation is documentation of internal control.

b. Program documentation provides a detailed analysis of the data used, the program logic, and the data produced.

c. Operator documentation (also called the "run manual") provides instructions for the computer operator on the use of the program (including required data files, startup instructions, check points, and program output).

Hardware Controls

.108 Necessary hardware controls are usually built into the equipment by the manufacturer and include parity checks, echo checks, and read-after-write checks.

Access Controls

.109 Access to program documentation, data files, programs, and computer hardware must be limited to the extent required by individual job duties. Access controls include the use of multi-level security, user identifications coupled with regularly changed passwords, limited access rooms, call backs and dial-up systems, use of file attributes, firewalls, and encryption of confidential data.

Safeguarding Records and Files

.110 The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) establish worldwide IT security standards that EISPD has adopted as the guide for creating an enterprise information security policy set for the State of Oregon. In accordance with EISPD Statewide Policy 107-004-052 Information Security, each agency shall develop and implement information security plans, policies and procedures that protect its information assets from the time of creation, through the useful life and through proper disposal. All plans and policies must include administrative, technical and physical safeguards to ensure the confidentiality, integrity and availability of agency information assets. In addition, each agency must identify, classify and manage its information assets based on the classification schema described in EISPD Statewide Policy 107-004-050 Information Asset Classification.

.111 Each agency shall physically control and protect portable and removable storage devices as well as protect and manage any sensitive information stored on them in accordance with EISPD Statewide Policy 107-004-051 Controlling Portable and Removable Storage Devices. In addition, any agency that sends, receives, or transports confidential or sensitve information to or from another agency is responsible for ensuring that the information is protected appropriately during transit from loss, destruction, or unauthorized access in accordance with EISPD Statewide Policy 107-004-100 Transporting Information Assets.

.112 Agencies must also take precautions to prevent accidental destruction of data. Control measures include the use of internal and external labels, file protection rings, boundary protection, and storing of key master files and records in safe places located away from the work site. It is recommended that copies of files kept on site be in fire-proof containers.

.113 Backup files must also be maintained. The process normally includes reading the previous file, recording transactions being processed, and then creating a new updated master file. The daily (or other interval) transactions are stored separately.

.114 Agencies are required to establish or be part of a disaster recovery plan for continuing operations in the event of destruction of not only program and data files, but also processing capability.

Application Controls

.115 Input control activities. Input controls are designed to provide reasonable assurance that data received for computer processing have been properly authorized and converted into machine-sensible form, and that the data have not been lost, suppressed, added, duplicated, or improperly changed. Computerized input controls include validation procedures such as check digits, record counts, hash totals and batch financial totals. Computerized edit routines include valid character tests, missing data tests, sequence tests and limit or reasonableness tests which are all designed to detect data conversion errors. Various input controls that may be imposed during data entry are described below:

a. Validity tests make sure the code entered is an existing code.

b. Check digits are created by subjecting characters of a field to an arithmetic algorithm. The algorithm yields a single digit that is then appended to the end of a field.

c. A field check verifies that data entered is of acceptable type (e.g., alphabetic, numeric, a certain number of characters, etc.).

d. A limit test checks to see that a numeric field does not exceed a specified limit.

e. A reasonableness check determines whether data in two or more fields is consistent.

f. A sequence check verifies all items in a numerical sequence are present.

g. When loop verification is used, additional information is displayed to confirm correctness or a request is made for explicit confirmation (e.g., “Are you sure you want to delete this employee record? Yes or No.”).

h. Key verification is the re-keying of critical data in the transaction followed by a comparison of the two keyings.

i. Preprinted forms and preformatted screens reduce the likelihood of data entry errors by organizing input data in a logical manner and by using default values whenever possible.

j. Automated data capture eliminates manual data entry by using automated techniques (e.g., scanners).

k. Checkpoint/restart is a processing control whereby a periodic snapshot of all data files is taken. If a system failure occurs, only transactions occurring since the last checkpoint need to be processed.

.116 Processing control activities. Processing controls are designed to provide reasonable assurance that data processing has been performed as intended without any omission or double-counting. Many processing controls are the same as input controls, but they are used during the actual processing phases. These controls include run-to-run totals, control total reports, file and operator controls, such as external and internal labels, system logs of computer operations, and limit or reasonableness tests.

.117 Output control activities. Output controls are designed to provide reasonable assurance that processing results are accurate and distributed to authorize personnel only. Control totals produced as output during processing must be compared/reconciled to input and run-to-run control totals produced during processing. Computer-generated change reports for master files must be compared to original source documents for assurance that data is correct. The following control reports assist in ensuring accuracy and completeness of data processing:

a. Processing reports list all the transactions used to update master files.

b. Error listings report all transactions and/or batches that failed one or more input controls.

c. Application reports are formal, formatted, regularly scheduled reports, usually created by programmers for use by end-users.

d. Ad hoc reports are informal, one-time only reports used to furnish specific information requests. Ad hoc reports are generally limited to database environments and are obtained through query of the system.

.118 The external control group shall receive all data, ensure it is recorded, follow up on errors that occur during processing and verify the proper distribution of output. A list of authorized recipients and a log of report distributions must be maintained. End-user controls supplement the information systems organization controls by performing redundant checks of processing totals and reconciling the results to independently maintained records.

Automated Interfaces Linking Agency Financial Systems to SFMA

.119 Agencies that interface financial data from their own systems into the Statewide Financial Management Application (SFMA), which includes both R*STARS and ADPICS, are responsible for ensuring the transmitted data is timely, accurate, and complete. New interfaces and changes to existing interfaces are reviewed and approved by the Statewide Financial Management Services (SFMS) Analysis and Development (A&D) unit. Interfaces to SFMA are subject to testing and acceptance requirements as specified by the A&D unit.

.120 Approval to establish and continue using an automated interface also depends on an agency's ability to reconcile data maintained in its internal financial system to data interfaced and posted in SFMA. Agencies are responsible to perform reconciliation procedures as often as data is interfaced and at a level of detail sufficient to ensure all data was transmitted timely, accurately and completely. Each agency head is responsible for ensuring that any discrepancy between an agency's database and the official financial records in SFMA is promptly and appropriately resolved. When changes to SFMA are made, agencies are responsible to modify their interfaces to adapt to such changes. SFMS is responsible for timely notifying agencies of any changes to SFMA that may impact agency interfaces.

.121 State agencies that transmit data to SFMA are responsible for establishing and monitoring the security of their automated interfaces and ensuring the integrity of the data that is transmitted. These same requirements also apply to entities that host agency applications and control the storage and transmission of data between agency applications and SFMA. In order to protect the data integrity of SFMA, the State Controller's Division reserves the right to suspend or terminate agency interfaces, or take other remedial actions at the cost of the agency, if the agency does not correct interface errors or appropriately modify interfaces in a timely manner.

Automated Interfaces Linking Agency Time and Attendance Systems to OSPA

.122 Agencies that interface time and attendance data from their own systems into OSPA are responsible for ensuring the transmitted data is timely, accurate and complete. New interfaces and changes to existing interfaces are reviewed and approved by Oregon Statewide Payroll Services (OSPS). Interfaces are subject to testing and acceptance requirements prior to approval.

.123 The approval to establish and continue using an automated interface to transmit time and attendance data also depends upon an agency's ability to reconcile data maintained in its own time and attendance system to data and hours paid posted to OSPA. Agencies must perform reconciliations as often as data is interfaced and at a level of detail sufficient to ensure all data was transferred timely, accurately, completely and for the correct pay period. Each agency head is responsible for ensuring that time reporting discrepancies are promptly and appropriately resolved.

.124 When changes to OSPA are made that necessitate changes to the time and attendance interfaces, agencies are responsible for modifying their interfaces to adapt to such changes. OSPS is responsible for timely notifying agencies of any changes that might impact agency interfaces.

.125 State agencies that transmit data to OSPA are responsible for establishing and monitoring the security of their automated interfaces and ensuring the integrity of the data that is transmitted. These same requirements also apply to entities that host agency applications and control the storage and transmission of data between agency applications and OSPA. In order to protect the data integrity of OSPA, the State Controller's Division reserves the right to suspend or terminate agency interfaces, or take other remedial actions at the cost of the agency, if the agency does not correct interface errors or appropriately modify interfaces in a timely manner.

Third Party Service Organizations

.126 When IT services for financial and accounting processes are outsourced to a third party service organization, state agencies must determine whether a written service level agreement (SLA) needs to be established. The purpose of an SLA is to define expectations and responsibilities based on the agency's requirements and IT capabilities. Important areas in which roles and responsibilities may need to be formalized include security and confidentiality, program change control, availability, reliability, performance and processing requirements, support, capacity for growth, and backup and disaster recovery.

.127 Other important areas to consider when outsourcing IT include:

a. Agreement regarding the level of logical access contractors or other third party providers will have to system programming or data. While certain access to the application and data may be necessary for operational purposes, unrestricted access or access not known to the agency poses a risk to the integrity and confidentiality of the data and the system.

b. How the service provider will restrict access to system logs.

c. Agreement regarding how security violation reporting and follow-up will occur, including when incidents will be reported, who will be notified, who will conduct investigations, and who will be responsible for resolving security incidents or breaches.

d. Provisions to ensure that application source code and other critical system documentation is properly maintained in escrow to allow for continued operations if the provider prematurely discontinues its operations or experiences an unexpected disruption of service.

.128 Another important consideration centers on independent audit assurance. Any time a service organization hosts or processes data belonging to an agency, the agency must determine whether a provision is needed in the contract that requires the service organization to demonstrate that it has adequate controls and safeguards. This may be accomplished by requiring the service organization to undergo an annual audit conducted by the agency or its designees.

.129 Alternatively, the service organization may already be subject to an annual audit that would satisfy the requirement. *Statement of Auditing Standards (SAS) No. 70, Service Organizations*, provides guidance to enable an independent auditor to issue an opinion on a service organization's internal controls, including controls over IT and related processes. A formal report known as a Service Auditor's Report, which also includes the auditor's opinion, is issued to the service organization at the conclusion of the SAS 70 examination. The service organization then makes this report available to its customers who, in turn, provide it to their auditors (such as Secretary of State, Audits Division) for use in planning the audit of the financial statements.

.130 There are two types of SAS 70 Service Auditor's Reports. A Type I report contains the service organization's description of controls at a specific point in time. A Type II report not only includes the service organization's description of controls, but also includes detailed testing of the controls over the period specified. State agencies that pursue a SAS 70 examination need to request a Type II report.

OREGON ACCOUNTING MANUAL		Number 10.65.00.PO
Oregon Department of Administrative Services State Controller's Division	**Policy**	Effective Date July 29, 2003
Chapter **Internal Control**		.1 OF .1
Part **Approval of Proposed Fiscal Systems**		
Section		Approval Signature on file at SCD

Authority **ORS 291.015**
ORS 291.038
ORS 293.595

.101 The Oregon Department of Administrative Services (DAS), State Controller's Division will review all proposed development, acquisitions, or modifications of fiscal systems. For purposes of this policy, fiscal systems are defined to include subsidiary systems that interface into statewide systems which are used to record transactions related to revenues, expenditures, assets and liabilities; to record or control non-capital or capital assets; or to record or produce vouchers, checks, purchase orders, or invoices. Statewide systems managed by the State Controller's Division include the Statewide Financial Management Application (SFMA) and the Oregon State Payroll Application (OSPA).

.102 Because of the cost to develop a fiscal system and the requirement for data processing support, the State Controller's Division, in conjunction with the DAS Information Resources Management Division (IRMD), will review all proposals to determine:

a. The need for purchasing, modifying, or developing a new system or a system that will interface to SFMA or OSPA.

b. Whether or not the proposed system duplicates the functionality of an existing statewide system.

c. The availability of data processing support.

d. The advisability of using or modifying an available system.

e. Uniformity with other state systems.

f. Adequacy of controls and audit trail.

The decision to approve or disapprove the request will be made based on the above determinations. The State Controller's Division will retain formal documentation of the decisions made and will provide a copy of such documentation to the Secretary of State Audits Division for their information.

OREGON ACCOUNTING MANUAL		Number 10.65.00.PR
Oregon Department of Administrative Services State Controller's Division	**Procedure**	Effective Date July 29, 2003
Chapter	**Internal Control**	.1 OF .1
Part	**Approval of Proposed Fiscal Systems**	
Section		Approval Signature on file at SCD

Request and Approval Process

.101 Any request for purchasing, designing, developing, or modifying a fiscal system must be submitted to the State Controller's Division. The request should identify the need and include a cost benefit analysis. It must be submitted and approved prior to any commitment by an agency for procurement or before any work is done by the agency's own data processing personnel.

.102 The Chief Financial Office (CFO) will either provide preliminary approval or will disallow the agency request. The SCD may also suggest modifications to the request.

.103 Once the agency has received preliminary approval from CFO, it should submit the documentation for approval to the DAS Information Resources Management Division (IRMD) with a request for a cost estimate. IRMD will confirm the preliminary approval with CFO.

.104 After receiving IRMD's cost estimate, the Chief Financial Office is to determine the feasibility of the proposal and review the findings with IRMD. CFO will then notify the agency, by letter, whether the request is being approved or disallowed, or whether modifications are necessary.

.105 Information Technology (IT) projects for fiscal systems are major expenditures other than routine maintenance. Agencies must provide a detailed description of IT projects for fiscal systems in their base budgets on budget form 107BF14. A copy of the completed form must be provided to CFO and to the IRMD analyst (in addition to being included in the budget document) when the agency request document is submitted. (Refer to Budget and Policy budget instructions at http://www.oregon.gov/das/Financial/Pages/Budgetinstruct.aspx.)

OREGON ACCOUNTING MANUAL

Subject:	Accounting and Financial Reporting	**Number:**	10.70.00
Division:	Chief Financial Office	**Effective date:**	June 14, 2017
Chapter:	Internal Control		
Part:	Security Access to Central Financial Systems		
Approved:	George Naughton, Chief Financial Officer		Signature on file

PURPOSE: This policy outlines the process and assigns responsibilities for requesting security access to the state's central financial systems.

AUTHORITY: **ORS 291.015**
ORS 293.595
Statewide IT Policy 107-004-050
Statewide IT Policy 107-004-052

APPLICABILITY: This policy applies to all entities that access the statewide financial systems.

FORMS: Systems Security Access Request Forms

POLICY:

101. Agency management must develop control procedures that ensure the systems access granted to each user is appropriate and consistent with the user's job duties.

102. The Chief Financial Office, Statewide Accounting and Reporting Services (SARS), Systems Security team manages security access for the following central financial systems:

a. SFMA (Statewide Financial Management Application). This mainframe application includes:

- R*STARS (Relational Statewide Accounting and Reporting System)
- ADPICS (Advanced Purchasing and Inventory Control System)

b. OSPA (Oregon State Payroll Application) – a mainframe application.

c. The Datamart – a system that houses tables of data downloaded from:

- SFMA (R*STARS, ADPICS)
- OSPA
- PPDB (Position and Personnel Database)
- PICS (Position Information Control System)

Access to PPDB and PICS is addressed in paragraphs 120 and 121 of this policy.

103. The SARS financial systems security officers (SSO) validate agencies' requests for systems access, provide training to ASOs, conduct semi-annual security reviews, and participate in the Secretary of State's annual audit of the financial systems.

104. Systems access must be set at the minimum level needed for the user to perform assigned job duties.

105. *At a minimum*, each agency should designate two Agency Security Officers (ASO) for each financial system the agency uses – one to serve as the primary security officer and one to serve as the backup. Each ASO is expected to understand how the financial system(s) operates, be familiar with the security access screens (including profiles), and have the ability to verify user access

106. To designate a new ASO, or change/revoke existing authority, the agency CFO (or designate) completes and submits the ***Agency Security Officer Notification Form*** to the Systems Security team within one business day of the change event.

107. ASOs must:

- Review, approve, and process all valid requests submitted by agency management to add, modify, or revoke a user's access to the central financial systems.
- Actively participate in the statewide semi-annual security reviews.
- Attend statewide security training provided every two years by the Systems Security team.
- ASOs may **not** submit security requests for their own access.

108. ASOs must document all requests received from agency management to add, modify, or revoke a user's access. Maintain all security documentation for audit purposes a minimum of three years.

109. Upon the complete fulfillment of a personnel action -- related to the departure or position change of an employee -- within PPDB, the employee's access to the systems covered by this OAM are automatically revoked in an overnight process. However, if the agency determines that an employee's access needs to be modified or revoked, and it will not result in the **immediate and complete** fulfillment of a personnel action as described above, the agency must notify the ASO within two weeks of that determination. In turn, the ASO will have one business day, starting from their notification by the agency, to notify the Systems Security team via email at security.systems@oregon.gov to modify or revoke the employee's access, as applicable.

    Each agency is responsible for developing procedures to notify their ASO timely of a need to revoke a user's access that is not related to the immediate and complete fulfillment of a personnel action as described above.

110. All systems security request forms must be submitted electronically to the Systems Security team by the ASO authorizing the add/modify/revoke.

111. **Users must not allow other individuals to use their passwords or RACF ID.** The Systems Security team will immediately revoke access to all central financial systems for each person involved in a security violation. Agencies are responsible for taking corrective actions, including disciplinary measures, and must contact the Systems Security team via email at security.systems@oregon.gov for reinstatement requirements and instructions.

PROCEDURES

Requests for Standard Access to SFMA and OSPA

112. The ASO reviews each written request for user access received from management to ensure the request is consistent with the user's position and assigned job duties. The written request for access is the beginning of the security audit trail.

113. If the ASO has a security concern, the ASO notifies the user's manager and suspends processing until the concern is resolved.

114. Once the concern is resolved, the ASO continues processing the request. The ASO completes the ***SFMA and OSPA – Mainframe Access*** request form located on the SARS Systems Security website:

http://www.oregon.gov/das/Financial/Acctng/Pages/Syst-security.aspx

When completing the form, the ASO must provide the following information for each user:

- Full name of the individual as shown in the PPDB
- The user's RACF ID
- Agency number
- The user's active email address and phone number
- The desired action: Add, Modify, or Revoke
- The system(s) requested – by completing the applicable section(s) of the form
- A brief explanation of job duties that require the specific access requested for each system. (Example 'to process payments received from vendors')

115. The ASO signs the form electronically, enters the current date, and uses the 'submit by email' button provided to submit the form to Systems Security.

116. The Systems Security team will deny access if any required information is missing or not active. Requests are processed when received; early submissions and incomplete forms will be returned to the ASO for correction and resubmission.

Requests for Special View Access to SFMA (R*STARS only)

117. Access requests for statewide user classes (UC) require additional security documentation. Scan and email completed request forms to the Systems Security team at security.systems@oregon.gov. The original hardcopy is to be maintained by the agency.

- Statewide user classes 01-10, 36, 38, 39, 46, 50, 59, 65, 70, and 79-81 are restricted to SFMA analysts, SARS analysts and Secretary of State Auditors. The requesting agency's Division Administrator must authorize the access request. These user classes may not be active if the employee is in telework status. Email the Systems Security team to obtain the ***Statewide User Class Access*** request form. This form is not available on the SARS website.
- UC 78 allows the user to view all agencies' transaction records, including data classified as restricted and critical. Senior fiscal officers and ASOs must ensure that UC 78 requests are based on valid needs and that the level of access is consistent with each user's job duties. Completion of the ***User Class 78 - All Agency View Access*** form is required.

Requests for Datamart Access

118. **Datamart Standard Access**: The ASO completes and submits the required ***Datamart Standard View Access - SFMA and OSPA Tables*** request form for access. Upon activation, SFMA Datamart information is accessible even if OSPA Datamart is the only table requested.

119. **Datamart Special View Access:** Security level 3 (restricted) and level 4 (critical) data are not included in the standard Datamart view. The ASO must work with the agency's senior fiscal officer to ensure that each request to view sensitive data is consistent with the user's position and assigned job duties.

    Datamart Standard View access must be activated before a special view is requested. Completion of the ***Datamart Special View Access*** form is required.

120. **PPDB Standard View Access:** The Department of Administrative Services (DAS), Chief Human Resources Office, HR Systems Section manages access to the PPDB system and the related tables in the Datamart.

    Contact PPDB Security at Group.PPDB@oregon.gov for assistance.

121. **ORBITS/PICS Standard View access:** The DAS, Chief Financial Office, Statewide Audit and Budget Reporting Section (SABRS) manages access to ORBITS and PICS and the related tables in the Datamart.

    Contact the SABRS unit at ORBITS.Help@oregon.gov for assistance.

OSPA Only – Terminal Access and Web Reports

122. ASOs must specifically identify the computer terminals used for OSPA mainframe access and the level of access allowed.

123. ASOs submit email requests to add or delete OSPA terminals not linked to a specific employee's activation to security.systems@oregon.gov. The notification must include:

    - Four-digit terminal identification number
    - Agency number
    - Type of access: 'U' for update, 'D' for display
    - Report printer identification (if applicable)
    - Description of the terminal location

124. The DAS, Oregon State Payroll Services (OSPS) unit manages access to the OSPA web reports.

    Contact the OSPS Help Desk at OSPS.Help@oregon.gov for assistance.

Requests to Change or Reset Mainframe Passwords

125. When a RACF ID revokes for password issues, only the user can request reactivation. The RACF ID user emails DAS Enterprise Technology Services directly at DAS.RacfUserAdm@oregon.gov.

The request must include the following information:

- Full name of the individual as shown in the PPDB
- The user's RACF ID
- Indication that the request applies to the mainframe system
- Request a "resume" when the password is known but was entered incorrectly
- Request a "reset" when the password was forgotten or has expired

126. DAS Enterprise Technology Services verifies ownership of the RACF ID and sends a temporary password directly to the user.

127. Web-to-Host mainframe users manage their passwords by accessing the Customer Information Control System (CICS) website:

https://columbia.das.state.or.us:3025/cics/wtst/daswpscp/ .

Requests to Change or Reset Datamart Passwords

128. Datamart users may change passwords or request a password reset. Follow the instructions located on the Datamart User Maintenance Site:

https://dasapp.state.or.us/DatamartApp .

Security Reviews and Training

129. Semi-annual statewide security reviews are conducted electronically beginning in February and August of each year. The SSO first verifies ASO assignments with each agency's CFO or designate.

The assigned ASO receives system-specific reports for review and analysis along with verification forms. The ASO verifies the correctness of the access granted to the agency's users and checks with the users' managers to determine if the level of access is still appropriate.

The ASO completes the verification form for each report by signing, dating, and recording any security changes to existing access. The ASO must return all verification forms to the SSO by the specified due date. Agencies should retain copies of the access reports for reference purposes.

OREGON ACCOUNTING MANUAL

SUBJECT:	Accounting and Financial Reporting	**Number:** 10.75.00
DIVISION:	State Controller's Division	**Effective date**: October 1, 2010
Chapter:	Internal Control	
Part:	ACH Security	
APPROVED:	John Radford, State Controller	Signature on file at SCD

PURPOSE: This policy emphasizes the commitment of the Department of Administrative Services to protect the confidentiality, integrity and availability of vendors' banking information. It outlines the responsibilities of Statewide Financial Management Services (SFMS) and Oregon Statewide Payroll Services (OSPS), units of the State Controller's Division, the Information Systems and Services (IS&S) unit of the Operations Division, and the State Data Center (SDC).

AUTHORITY:
ORS 291.015
ORS 291.100
ORS 292.018
ORS 292.026
ORS 292.034
ORS 292.042 –292.067
ORS 292.346
ORS 293.348

APPLICABILITY: Employees of SFMS, OSPS, IS&S and the SDC.

DEFINITION: **Automated Clearing House (ACH):** A computerized facility that performs the clearing of paperless entries between member depository institutions. It is a batch process system that is destine for future settlement of transactions. The ACH will take the transaction information and store it until necessary for payment to occur on the settlement date.

POLICY:

101. ACH security awareness is the responsibility of senior management. SFMS, OSPS, IS&S and the SDC are responsible for this security with respect to their roles in handling and storing the ACH information related to state disbursements. Ultimately, every user has a responsibility to safeguard the ACH information to which they have access.

102. Management must ensure that the agency protects ACH information appropriately based on the sensitivity of the information.

103. Management must ensure that every employee under their direct supervision who has access to ACH information is aware of this policy.

104. Management must provide appropriate training and ensure that only employees with ACH duties have access to banking information. Management must implement internal safeguards to hold users accountable for their actions. See Information Security Statewide Policy #107-004-052.

PROCEDURES:

105. SFMS employees must develop policies and procedures to ensure that the classification, labeling and handling of documents that contain personally identifiable banking information are kept secure at all times. This includes the Direct Deposit Authorization Form, Statewide Financial Management Application (SFMA) control reports, screen prints of vendor profiles and any other communication, including electronic communication that may contain sensitive information. Currently, e-mail is not secure but the SFMS fax machine is.

    a. SFMS employees must provide IT staff with direction on appropriate asset classification levels, including special handling during disposal of electronic files. All ACH data is asset classification level 4.

    b. SFMS employees must perform an annual ACH risk assessment and deliver this assessment to Treasury by December 31.

    c. SFMS employees must develop and test an ACH incident response policy.

106. OSPS employees must develop policies and procedures to ensure that the classification, labeling and handling of documents that contain personally identifiable banking information are kept secure at all times. This includes direct deposit authorizations, Oregon Statewide Payroll Application (OSPA) reports, table-change documentation, screen prints and any other communication, including electronic communication that may contain sensitive information. Currently, e-mail is not secure but the OSPS fax machine is.

    a. OSPS employees must provide IT staff with direction on appropriate asset classification levels, including special handling during disposal of electronic files. All ACH data is asset classification level 4.

    b. OSPS employees must perform an annual ACH risk assessment and deliver this assessment to Treasury by December 31.

    c. OSPS employees must develop and test an ACH incident response policy.

107. IS&S employees must develop policies and procedures to ensure that SFMA and OSPA electronic data files that contain personally identifiable banking information are not inappropriately accessed and are not altered without approval from SFMS or OSPS management. When available, management must ensure that audit trails and intrusion-detection reports are reviewed on a regular basis.

108. SDC employees must develop policies and procedures to ensure that the electronic data files that contain personally identifiable banking information stored on the SDC's mainframe are secure from internal and external threats. SDC employees are responsible for following SFMS and OSPS' guidance on data classification levels related to data storage and deletion. See Information Asset Classification Statewide Policy #107-004-050. SDC is responsible for preventing the threat and risk of data intrusion from outside sources

109. See additional statewide policies published by the Enterprise Security Office at http://www.oregon.gov/DAS/OSCIO/Pages/Security.aspx .

Authority **ORS 291.015**
ORS 291.026
ORS 291.040
ORS 293.515
ORS 293.590

Auditor Understanding of Internal Control

.101 The Secretary of State, Audits Division, is the constitutional auditor of public accounts in Oregon. The Audits Division conducts a statewide single audit annually, and performs other audits and reviews at its discretion. The audits are performed in conformance with generally accepted government auditing standards.

.102 Generally accepted auditing standards require that the independent auditor study and evaluate the existing system of internal control as a basis for reliance thereon to determine the nature, timing, and extent of tests to be performed. Findings and judgments resulting from the auditor's study of internal control affect the overall audit plan including judgments about staffing, extent of supervision, conduct and scope of the audit, and degree of professional skepticism applied.

.103 Internal auditors provide assistance to independent auditors by documenting existing systems and controls, recommending appropriate corrective actions, and assuring recommendations are implemented as planned. The Audits Division may rely upon the work of internal auditors in certain circumstances.

Federal Compliance

.104 Agency management is required to identify laws and regulations pertaining to compliance requirements. Agencies should establish internal controls to ensure compliance with those laws and regulations applicable to federal assistance.

Financial Statement Compliance

.105 Agency management is required to establish internal controls to ensure compliance with laws, regulations, and provisions of contracts and grant agreements that have a direct and material effect on the determination of financial statement amounts.

Entrance and Exit Conferences

.106 **Agency heads** or their designees must attend the audit entrance and exit conferences.

Agency Responsibility to Respond to Audit Findings

.107 For all audits conducted by, or under the auspices of, the Audits Division, agency management is responsible to respond to audit findings and ensure proper resolution.

Audit Sanctions

.108 ORS 293.515 allows the Secretary of State to certify to the Governor the failure of State officials or employees to comply with significant recommendations in audit reports.

a. The Governor may or may not order compliance with the audit recommendations.

b. The Governor may order withholding of salaries in order to obtain compliance with orders issued.

Statewide Single Audit

.101 Single audits have three layers of audit standards with different reporting requirements.

a. **Generally Accepted Auditing Standards** (GAAS)

(1) An opinion is made on the financial statements and supplementary **schedule of expenditures of federal awards** (SEFA).

(2) A report on internal control is made only if reportable conditions are discovered. Oral reporting is acceptable.

b. **Generally Accepted Government Auditing Standards** (GAGAS)

(1) An opinion is made on the financial statements and the schedule of expenditures of federal awards.

(2) A report on compliance and on internal control over financial reporting is made based on the financial statements.

(3) A report on internal control is required in every financial statement audit and must be in writing.

c. Federal Office of Management and Budget **(OMB) Circular A-133**

(1) An opinion is made on the financial statements and the supplementary schedule of expenditures of federal awards.

(2) A report on compliance and on internal control over financial reporting is made based on the audit of financial statements.

(3) A report on compliance and on internal control over compliance applicable to each major program (as defined in circular A-133) is made, including an opinion on compliance.

(4) A schedule of findings and questioned costs is required. ("Questioned costs" are expenditures deemed to be non-allowable for reimbursement under a federal grant.)

(5) A report on internal control is required in every financial statement audit and must be in writing.

.102 The State and its agencies are responsible to comply with the provisions of the **Single Audit Act**, as amended, to ensure that the State continues to be eligible to receive federal funding. See **OAM 30 10 00** on federal compliance.

.103 Within 180 days of the fiscal year ended June 30, Statewide Accounting and Reporting Services will issue a **Comprehensive Annual Financial Report (CAFR)**. The CAFR will include an audit opinion as to whether the State has presented fairly its financial position and the results of its financial operations in accordance with generally accepted accounting principles. The Audits Division will conduct the Statewide Single Audit.

.104 The State and its agencies are generally subject to a variety of laws and regulations that affect the Comprehensive Annual Financial Report and agency financial statements. Such laws and regulations may address fund structure, required procurement, debt limitations, and legal authority for transactions.

a. Management responsibilities are to:

(1) Identify applicable laws and regulations with compliance requirements.

(2) Establish internal controls to provide reasonable assurance that the entity complies with those laws and regulations.

(3) Prepare supplementary financial reports, including a schedule of expenditures of federal awards.

b. Auditor responsibilities are to:

(1) Obtain reasonable assurance that the financial statements are free of material misstatements resulting from violations of laws and regulations that have a direct and material effect on the determination of financial statement amounts.

(2) Obtain an understanding of the possible effects on financial statements of laws and regulations that are generally recognized by auditors to have a direct and material effect on the determination of amounts in the entity's financial statements.

(3) Assess whether management has identified laws and regulations that have a direct and material effect on the determination of amounts in the entity's financial statements.

(4) Obtain an understanding of the possible effects on the financial statements of the laws and regulations identified by management.

Performance Audits

.105 Performance audits such as economy and efficiency audits determine whether the entity makes efficient use of resources. The audits determine the following:

a. Whether the agency is acquiring, protecting, and using its resources economically and efficiently.

b. The causes of inefficiencies or uneconomical practices.

c. Whether the agency has complied with laws and regulations on matters of economy and efficiency.

.106 Program audits, another example of performance audits, determine the effectiveness and measure the achievement of a program. The audits determine the following:

a. The extent to which the desired results or benefits established by the authorizing body are being achieved.

b. The effectiveness of agencies, programs, activities, or functions.

c. Whether the agency has complied with laws and regulations applicable to the program.

Responding to Audit Findings

.107 Agencies are responsible for assuring the adequacy, effectiveness, and timeliness of actions taken with respect to reported audit findings, both from internal auditors and from the Audits Division.

.108 For those agencies without internal audit functions, the State Controller's Division, subject to resource availability, may follow up to verify progress on resolution of audit findings.

Accountability and Control Standards

.101 This policy sets accountability and control standards for the determination and delegation of review and approval authority for the agency head's monthly time report, requests for vacation payoff, use of exceptional performance leave, travel expense reimbursement claims, and Small Purchase Order Transaction System (SPOTS) card purchases. This policy is intended to ensure that these transactions are reviewed for completeness and accuracy and that they are in conformance with and measured against the documentation and compliance standards provided herein. In the case of agency heads that are elected, this policy may be applied at the option of that elected official.

Establishing Review and Approval Authority

.102 Agency heads appointed by the Governor shall delegate review and approval authority for agency head financial transactions to the chief financial officer or to the person who holds the position of second-in-command to the agency head. The delegation shall be in writing.

Agency heads appointed by or reporting to a board or commission shall work with that body to create a review and approval structure for financial transactions of the agency head. The board or commission may delegate the review and approval authority, by direct designation or motion, in writing, to the board or commission chair or ranking officer. Or, the board or commission may delegate to the agency second-in-command, chief financial officer, or may choose to retain an active role in the approval process. Boards and commissions choosing to take an active role in the review and approval process must make the review and approvals of financial transactions a part of their regular meetings and document them in the minutes.

Boards and commissions delegating the review and approval process must at least annually review the financial transactions of the agency head approved as delegated. These post transaction reviews and approvals must be documented in the minutes of the board or commission annual meeting.

Requirement for Internal Procedure and Review

.103 This policy requires agencies to develop internal procedures for the review and approval of the following agency head transactions:

(a) Time reporting: Review and approve the agency head's monthly report of sick leave, vacation, holiday or other leave hours used. Review for completeness and accuracy and to ensure that all time that has been taken has been reported. Ensure that leave hours comply with HRSD 60.000.01 Sick Leave, 60.000.05 Vacation Leave, 60.010.01 Holidays, 60.000.15 Family Medical Leave, 60.005.01 Leave Without Pay and 60.000.10

Special Leaves with Pay. Time reporting (leave usage) must be documented using either paper or electronic timekeeping methods. The documentation must show that the time reports have been reviewed and approved by the appropriate authority, which, in the case of a board or commission, may be the ranking officer of the board. Note: Heads of agencies are classified as exempt from the Fair Labor Standards Act (FLSA) and as such should not be required to report actual hours worked. The time reporting review is intended to focus only on hours related to the categories defined above. The documentation must provide evidence for an audit trail and must be maintained by the agency for the prescribed IRS retention schedule for time records of three years and one quarter as well as the current record retention standards per Secretary of State, Archives Division.

(b) Travel expense reimbursements: Review and approve all travel claims submitted by the agency head, whether for in-state or out-of-state travel. Ensure compliance with DAS Travel Rules **OAM 40.10.00** as well as **OAM 10.40.00**, Expenditures. The review and approval of travel transactions must be documented to provide an audit trail and evidence that the review complies with and was conducted in accordance with the prevailing state policies as listed.

(c) Exceptional Performance Leave: This leave shall be granted to agency heads using the criteria set forth in HRSD 60.000.10 “Special Leaves With Pay”. For agency heads appointed by the Governor, this leave shall only be granted by the Governor or by the Director of the Department of Administrative Services on behalf of the Governor. For agency heads reporting to a board or commission, this leave shall be granted by that body or by the board or commission chair and documented in the minutes of the board or commission. The review and approval responsibility is to ensure that the Exceptional Performance leave was granted based on appropriate criteria and authority and is in compliance with HRSD policy 60.000.10. The review and approval of these transactions must be documented to provide an audit trail and evidence that the review complies with and was conducted in accordance with the prevailing state policies as listed. The documentation must clearly demonstrate the criteria upon which the leave was granted. The documentation must include copies of the written request and approval granting the leave and copies of the board or commission minutes, if applicable. The documentation must be retained according to the current record retention standards per Secretary of State, Archives Division.

(d) Vacation Payoff: Review and approve ensuring compliance with HRSD policy 60 000.05 “Vacation Leave”. The review and approval of these transactions must be documented to provide an audit trail and evidence that the review complies with and was conducted in accordance with HRSD 60.000.05. That review must clearly demonstrate that the vacation payoff was approved in accordance with Section (6)(b) of that policy which mandates that a vacation payoff is only granted when taking vacation leave is not appropriate. Copies of the written request and approval granting the vacation payoff and copies of the board or commission minutes, if applicable, must be part of the documentation for these transactions.

(e) Use of the Small Purchase Order Transaction System (SPOTS) purchase card: Review purchases to ensure that they are appropriate expenditures that further the business of the state and the mission of the agency and that the use of the SPOTS card complies with **OAM 55.30.00**. The review must be conducted by someone other than the person whose name appears on the card. The review and approval of transactions must be documented to provide an audit trail and evidence that the review complies with and was conducted in accordance with the prevailing state policies as listed.

The documentation for all of the above should be retained according to the current record retention standards per Secretary of State, Archives Division.

Fiscal Officer Responsibility

.104 Agency fiscal officers processing these financial transactions for the agency head have a duty to pre-audit and verify that the transactions comply with this policy.

Seeking Guidance from Chief Financial Office

.105 For the purposes of this policy, those persons delegated to review and approve financial transactions for state agency heads have a duty to comply with the provisions of this policy. Any agency head requests to deviate from this policy must be approved by the Chief Financial Officer. Those persons delegated review and approval authority that have reservations or questions about an agency head financial transaction may seek guidance from the Chief Financial Office.

Transactions Subject to Audit

.106 All financial transactions of state agency heads are subject to periodic audit by the Secretary of State Audits Division.