DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

Statewide Policy

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 .