


OREGON ACCOUNTING MANUAL

 STATEWIDE POLICY	NUMBER 10.75.00	SUPERSEDES 10.75.00 dated 10/01/2010
	EFFECTIVE DATE MM/DD/YYYY	PAGE NUMBER Pages 1 of 3
Division Chief Financial Office	REFERENCE/AUTHORITY ORS 291.015 ORS 291.100 ORS 292.018 ORS 292.026 ORS 292.034 ORS 292.042 –292.067	
Policy Owner Statewide Accounting and Reporting Services		
SUBJECT Internal Control - ACH Security	APPROVED SIGNATURE <i>George Naughton, Chief Financial Officer</i> Signature on file	

PURPOSE

The purpose of this policy is to emphasize the commitment of the Department of Administrative Services to protect the confidentiality, integrity and availability of banking information. It outlines the responsibilities of Statewide Financial Management Services (SFMS), Oregon Statewide Payroll Services (OSPS), Chief Human Resources Office Workday (CHRO WD), the Application Delivery (AD) unit of DAS IT, and the Data Center Services (DCS).

APPLICABILITY

This policy applies to employees of SFMS, OSPS, CHRO WD, AD and DCS.

FORMS/EXHIBITS/INSTRUCTIONS

DAS statewide policies:

- Information Asset Classification (107-004-050) <https://www.oregon.gov/das/Policies/107-004-050.pdf>
- Cyber and Information Security (107-004-052) <https://www.oregon.gov/das/Policies/107-004-052.pdf>
- Statewide policies published by Cyber Security Services
<https://www.oregon.gov/das/Pages/policies.aspx#IT>

DEFINITIONS

Automated Clearing House (ACH): A computerized facility that performs the clearing of paperless entries between member depository institutions. It is a batch process system 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.

Click here for other [definitions](#).

EXCLUSIONS AND SPECIAL SITUATIONS

None.

POLICY:

101. ACH security awareness is the responsibility of management in each of the listed sections. SFMS, OSPS, CHRO WD, AD and the DCS 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 with access to ACH information reads 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. Refer to Statewide Policy Cyber and Information Security (107-004- 052).

PROCEDURES:

105. SFMS, OSPS and CHRO WD employees must develop separate policies and procedures to ensure the classification, labeling and handling of documents that contain personally identifiable banking information are kept secure at all times. This includes Direct Deposit Authorization Forms, system control reports, screen prints of profiles, table change documents and any other communication, including electronic communication that may contain sensitive information. Currently, email is not secure.
 - a. SFMS, OSPS and CHRO WD management 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 3.
 - b. SFMS, OSPS and CHRO WD management must each perform an annual ACH risk assessment and deliver an attestation letter to Oregon State Treasury by December 31.
 - c. SFMS, OSPS and CHRO WD management must develop and test an ACH incident response policy.
106. AD must develop policies and procedures to ensure that Statewide Financial Management Application (SFMA) and Oregon State Payroll Application (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, SFMS and OSPS management must ensure that audit trails and intrusion-detection reports are reviewed on a regular basis.
107. CHRO WD must ensure their service provider develops policies and procedures to ensure Workday electronic data files that contain personally identifiable banking information are not inappropriately accessed and are not altered without approval from CHRO WD management. When available, CHRO WD management must ensure that audit trails and intrusion-detection reports are reviewed on a regular basis.

108. DCS must develop policies and procedures to ensure electronic data files that contain personally identifiable banking information stored on the DCS mainframe are secure from internal and external threats. DCS employees are responsible for following SFMS and OSPS guidance on data classification levels related to data storage and deletion. Refer to Statewide Policy Information Asset Classification (107-004-050). DCS is responsible for preventing the threat and risk of data intrusion from outside sources.
109. CHRO WD must ensure their service provider develops policies and procedures to ensure electronic data files that contain personally identifiable banking information stored on the service provider's hardware are secure from internal and external threats. The service provider is responsible for following WD guidance on data classification levels related to data storage and deletion. Refer to Statewide Policy Information Asset Classification (107-004-050). The service provider is responsible for preventing the threat and risk of data intrusion from outside sources.

DRAFT