

Client Agency Policy & Operations Manual

SECTION: 20 General Administration

NUMBER: SCS-20-010

TITLE: Use of State Technology, Systems & Components

EFFECTIVE DATE: 3-13-02

APPROVED: Signature on file with the State Controller's Division

**PURPOSE and/or
RESULTS DESIRED:**

This policy is designed to assure technology used by client agencies is in alignment with state standards, system security is maintained, and resources are used in a reasonable manner.

AUTHORITY:

[ORS 291.015](#) Fiscal responsibilities of department; delegation of fiscal functions.
[ORS 293.590](#) Department to supervise state agency accounting; furnishing accounting services.
[ORS 293.595](#) Supervision of data processing equipment for accounting system; other uses.
[OAM 10.10.00 PO](#) Management's Responsibilities.
[OAM 10.60.00 PO](#) Information Technology.
[DAS-IRMD Oregon Statewide IT Policy.](#)

APPLICABILITY:

Client agencies assigned and/or contracting for accounting, budgeting, and financial reporting services with the State Controller's Division, DAS.

DEFINITIONS:

Information technology includes, but is not limited to, any systems, components, devices, or services utilized for the purpose of telecommunication, data processing, or office automation.

POLICY:

Each client agency head has responsibility for establishing, maintaining, and improving internal controls over agency Information Technology (IT).

GUIDELINES:

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

- A. Design, implementation, and operation of agency IT internal control should be adequate to provide an acceptable level of confidence in the system and assurance that:
- Management's IT goals and objectives are being accomplished effectively and efficiently;
 - IT investments and investment strategies are well planned and adequately funded;
 - IT assets are safeguarded; and
 - IT operational and investment strategies are executed in accordance with management's direction, authorization, and security and control policies.

- B. Client agencies should provide adequate IT security and control training and educational support to client agency employees involved in the design, development, implementation, maintenance, and management of their IT infrastructure programs. Training is available through a variety of nationally and locally recognized professional associations and through the Department of Administrative Services – [IRMD Division](#).
- C. Client agencies should be aware that the Audits Division has adopted Control Objectives for Information and Related Technology (CobiT) standards, which is published by the Information Systems Audit and Control Foundation (ISACF), as the basis for auditing the IT management function.
- D. Client agencies should comply with the appropriate IT management policies and guidelines established by DAS IRMD. Copies of CobiT may be obtained at <http://www.isaca.org/>.

II. Personal Use Restricted

- A. Employees are needed to remain at work despite personal needs and interests. It is also necessary for employees to continuously develop their knowledge and skills. For those reasons, certain personal uses of systems may be allowed.
 - 1. Personal use of agency systems must be at no cost to the agency.
 - 2. Examples of allowed personal uses:
 - Sending and receiving personal e-mail.
 - A short incoming or outgoing local fax.
 - 3. Examples of allowed mixed state and personal uses:
 - Printing and photocopying a state job application, resume or personnel papers.
 - Printing and photocopying material for agency authorized courses of study.
 - 4. Examples of personal uses that must be reimbursed:
 - Copying or printing personal papers.
 - 5. Examples of personal uses not allowed:
 - Outgoing, long-distance fax's; and
 - Toll calls.

III. Information Technology Security

- A. The Client Agency Head shall develop and implement policies and procedures designed to maintain the security of IT systems, components and any related confidential or sensitive information.
- B. Internal system safeguards, at a minimum, should address the following:
 - 1. **Accountability.** Users are held accountable for their actions. Users who fail to follow mandatory requirements for IT security may be subject to personnel action or dismissal.
 - 2. **Virus protection.** Virus prevention by employing basic anti-virus practices such as using virus prevention software and using only authorized application software.
 - 3. **Report of suspicious activity.** Users must report suspicious activity to the agency head. Suspicious activity includes suspected misuse of government resources; use of system by unauthorized party; illegal copying of software; or strange activity on a computer system which may be caused by a computer virus or other malicious logic.
 - 4. **Electronic Mail.** Electronic mail is primarily for business use. It is not be used

for distribution of confidential information. It is not private and may be accessed by the state at any time.

5. **Security training and awareness.** The Client Agency Head shall establish a security training and awareness program that will ensure all users who are responsible for IT systems or information are aware of proper operational and security-related procedures. Training may be delivered formally or through written communication.

IV. Internal Control and Risk Management

- A. The Client Agency Head is responsible for establishing, maintaining and improving the agency internal control of all information technology systems, components, and devices. All systems and information are, and shall remain, the property of the agency, subject to its sole control. No part of the system or information is, or shall become, the private property of any system user. The agency owns all legal rights to control, transfer, or use all or any part or product of its system. All users must comply with this policy and with all other state policies and rules that apply.
- B. Internal control
 1. The agency reserves all rights relating to information used in its system.
 2. The agency may trace, review, audit, access, intercept, block, restrict, screen delete, recover, restore, publish, or disclose any information, at any time without notice, as permitted by law.
 3. The agency may withdraw permission for any personal or business uses of its systems at any time without cause or explanation. No one shall grant access to systems without agency authorization.
- C. Risk assessment
 1. Risks are potential costs or undesirable results from weaknesses in the internal control of an agency. Risks include external and internal events or circumstances that may occur and adversely affect operations.
 2. When adopting, developing, or issuing any IT system, component, or device the agency head should identify and consider any risks associated with its use and any potential misuse.
 3. Once risks are identified, management should consider their significance, the likelihood of their occurrence, and how to manage them. Management should initiate plans, programs, or actions to address specific risks.
- D. Monitoring
 1. Monitoring is the process that assesses the quality of internal control performance over time, by assessing use and operation of IT systems on a timely basis and taking necessary corrective actions.
 2. The monitoring process should include ongoing activities built into regular management and supervisory activities.
- E. Use of agency IT
 1. Use must reflect agency image.
 2. Use must be lawful and inoffensive.
 3. Use must be agency authorized.

4. A user may not put to his or her personal use any system device that the user does not employ in his or her assigned work. No privately owned device may be connected to state systems without agency authorization. System devices taken home or otherwise used outside of the worksite remain subject to this policy.
 5. Employees may make limited personal use of their assigned information technology tools. Personal use should be at no cost to the agency.
 6. Any actual cost incurred during the personal use of agency IT systems must be reimbursed by the user.
 7. No personal use may be made by, or on behalf of, any organization or third party.
- F. Agency information technology systems, components and devices includes, but is not limited to, any property paid for and/or provided by the state to the employee for the purpose of telecommunication, data processing or office automation. Examples of agency IT systems, components and devices include:
- Desktop telephones;
 - Cell phones;
 - Pagers;
 - Personal computers;
 - Laptop computers;
 - Copiers, Printers;
 - Parking keys;
 - Recorders;
 - Transmitters; and
 - Other systems accessed through IT devices (i.e. Internet, e-mail, cable television, and phone services).

V. Acknowledgments and Conflicting Provisions – The agency will ensure all employees are informed of the IT security policies and procedures. A valid collective bargaining agreement shall supersede any conflicting terms in this policy.

FORMS:

Sample Computer User Security Declaration – ATTACHED.

