03-6-1104-014

Date: October 29, 2003

Rec'd 11/4/03

Approved: _____
SAM S. REED
Secretary of State

POLICY ON OSOS Network Use

APPROVED
Executive Ethics Board
Date: 1/12/04

Authority

42.52 RCW (Ethics in Public Service Act)
WAC 292-110-010 (Use of State Resources Rule)
OSOS Use of State Resources Policy
OSOS Policy Against Harassment
OSOS Discrimination Complaint Policy and Procedures
OSOS Policy on Preventing Workplace Violence

Purpose

This policy sets forth guidelines defining the limits of permitted uses of the computer network resources by employees and volunteers of the Office of the Secretary of State.

Applicability

This policy applies to all employees and volunteers of the Office of the Secretary of State (OSOS).

Overview

Successful operation of the OSOS computer network requires that all users conduct themselves in a responsible, ethical and polite manner while using the network. The OSOS network is available for use in support of the business, operation, and research of the Office of the Secretary of State. It is a state resource, and as such, its use is governed by office policies and applicable state laws and regulations dealing with the appropriate and ethical use of state resources. Limited and occasional personal use will be governed by the Use of State Resources Policy, in addition to this policy. Use of OSOS network resources should not reflect poorly on the OSOS nor should it interfere with job performance.

Definition

Network: includes personal computers (PC), laptops, printers, fileservers, Email, Internet connection, peripherals, and other electronic resources.

Assigns audits and/or inspections of employee use of network.

APPROVED
Executive Ethics Board
Date: 1/12/04

APPROVED
Executive Ethics Board
Date: 1/12/04

Policy

1. Supervisors assign network resources to employees.

Supervisor ensures that employee has equipment necessary to carry out the employee's assigned duties. As appropriate, supervisor contacts the IT group to arrange for individual user network logon name and password assignments.

2. Each employee responsible for authorized use of his/her logon name and password.

Because the agency uses a single sign-on strategy to access multiple computer platforms/resources, each user is responsible for the security of his/her logon name and password and any unauthorized use associated with the logon name and password. Users are not permitted to share logon names, passwords, or gain access to any network or application through the frivolous use of someone else's logon name or password. An exception would be the need to access agency work products or instructions in the absence of the authorized user.

3. All software approved by OSOS IT management.

Prior to deployment on any agency PC, all software must be approved for use on the OSOS network. Unless otherwise delegated by the division director and approved by IT management, downloading and installing unauthorized software from the Internet, including "plug-ins", updates to existing software, "shareware", "freeware", or "alpha/beta" versions of programs will not be allowed. Employees shall not intentionally upload or Email files or programs that can cause harm to other networks or systems ("viruses", "bombs", "worms", etc.).

4. Use of Personal Data Assistants (PDAs) must be approved.

Because PDAs allow personal data from a remote computer to become downloaded into the agency's network, their use must be approved by the Assistant Secretary of State or Deputy Secretary of State. Personal Email and calendar appointments that are introduced through use of an approved PDA will be considered to be an appropriate limited and occasional use of state resources, and, as such, are approved under this policy as well as the OSOS Use of State Resources Policy.

5. Email used for business purposes only, with occasional and limited exceptions.

The agency's Email system is to be used for transmitting, receiving, and storing information for business purposes. Use of the Email system or instant messaging for personal communications, either within the agency or to persons outside the agency, must be occasional and limited as spelled out in the OSOS Use of State Resources Policy.

Communications that support organizational effectiveness and do not undermine public trust and confidence, such as items relating to agency-sponsored sports activities, announcements about personnel (e.g., newborn children), invitations to agency

APPROVED
Executive Ethics Board
Date: 1/12/04

Procedures:

Responsible Party:	Actions:
Supervisor	Contacts IT Group to arrange for individual user network logon name and password for new employee if network access is required to carry out assigned duties. Notifies IT Group when an employee leaves employment or access to network is no longer needed so logon and password can be eliminated.
	Ensures that employee is aware of this policy and monitors employee's compliance to the extent possible. Answers questions related to appropriate use. Approves/denies specific uses upon request.
	Authorizes access to agency work products or instructions using employee's logon in employee's absence
	If has reason to believe that employee may have violated network use policy, submits written request to Division Director to review employee use of the network.
Employee and volunteers authorized to use network	Understand and follow the guidelines contained in this policy.
	Protect security of assigned password.
Division Director	Approves all software use on the OSOS network prior to deployment.
	Determines whether to forward supervisor's request to review employee use of the network to IT Management. If so, sends copy of request to OSOS HR Office as well.
	In conjunction with HR, initiates any formal corrective/disciplinary actions resulting from employee inappropriate use of network.
IT Group Member	Upon notification by agency supervisors, performs needed actions to establish or delete employees' network logon names and passwords.
IT Management	Upon request by Division Director, arranges for the supervisor's viewing of the employee's network use history.
	Upon request of Assistant Secretary of State or Deputy Secretary of State arranges for audits and/or inspections of employee use of the network.
Agency Webmaster	Maintains and monitors content and publication of materials on the World Wide Web site. Establishes standards for WWW publication and infrastructure.
Asst Sec of State or Deputy Sec of State	Approves use of PDAs.

functions, safety alerts, etc., are appropriate on an occasional and limited use basis. Inappropriate Email would include soliciting the sale of personal items, requests for contributions for personal charities, or participation in outside activities unrelated to the agency's business. Email messages that include obscene statements or contain derogatory comments about the agency, co-workers, clients, or others with whom the agency does business should never be created or transmitted. Evaluatory comments received or created by supervisors or managers in the course of preparing employee evaluations or counseling employees on performance issues are an approved use and would not be considered to be prohibited derogatory comments.

6. Certain uses of OSOS network resources specifically prohibited.

An employee may not use network resources to (applies as well to network resources removed from state facilities):

- Interfere with or disrupt other network users, services, data, or equipment;
- Gain or communicate passwords belonging to other users;
- Use or knowingly allow another to use the OSOS network to devise or execute a scheme to defraud or obtain anything of value by false pretenses, promises, or representations;
- Engage in any activity prohibited by OSOS Policy Against Harassment;
- Transmit or view material with sexual content;
- Promote or engage in discrimination on the basis of race, color, sex, religion, creed, age, marital status, national origin, sexual orientation, disability or veteran status;
- Conduct political campaigns or other personal political use;
- Conduct a personal outside business or private employment;
- Engage in gambling or other activity resulting in personal gain;
- Support, promote or solicit on behalf of an outside organization;
- Buy, sell, or advertise a product unless it is job related;
- Infringe on any copyright (including the unauthorized use of and/or copying of software); or,
- Promote or engage in any illegal activity.

APPROVED
Executive Ethics Board
Date: 1/12/04

7. Network resources belong to OSOS – no expectation of privacy.

No one in the agency has a right to privacy in any matter created, received, or sent on the OSOS network. The agency may audit, inspect, log, and/or monitor employee use of the Internet and will be able to identify web sites visited by individual employees. Email messages and other electronic communications may be accessed and reviewed by systems or other agency personnel, notwithstanding the use of passwords. Employees should not say anything in Email that would not be appropriate to record in

a typewritten memo or letter. Information transmitted or stored on Email, hard drives, servers, or other electronic resources within the OSOS network is the sole property of the agency.

8. OSOS World Wide Web site managed through Agency Webmaster.
The Agency Webmaster coordinates updates to the OSOS home page. Divisions desiring the ability to maintain their portion of the OSOS home page will coordinate through the Webmaster.

9. Questions concerning appropriate use directed to Supervisors.

Employees who wish to send an Email within the agency or use OSOS network resources and who are uncertain about whether it is permitted under these guidelines, should discuss the matter first with a supervisor. Employees may request explicit approval from a supervisor regarding a particular use of network resources. If an employee or supervisor has any doubt about whether a contemplated use is allowable, the best guidance would be to opt not to use.

10. OSOS not liable for loss due to reliance on OSOS Network.

The OSOS will strive to provide error free and dependable access to technology resources associated with the OSOS network. However, neither the OSOS, nor any division, program, employee, or consultant of the office warrants the accuracy, reliability or timeliness of any information available through the OSOS network and shall not be held liable for any losses caused by reliance on the accuracy, reliability or timeliness of such information.

11. Access to Network resources may be restricted or removed.

An employee's access to network resources may be restricted or removed at any time it is determined that the employee is engaged in unauthorized activity, is in violation of this policy, or access to network resources is no longer required to carry out their job duties.

12. Violation of policy may be grounds for disciplinary action.

Violation of this policy may be grounds for disciplinary action up to and including termination and/or appropriate legal action. Exact disciplinary measures will be consistent with OSOS standard policies and practices and will be determined on a case-by-case basis.

APPROVED
Executive Ethics Board
Date: 1/12/04