



# Acceptable Use of Electronic Systems Policy

Subject Acceptable Use of Electronic Systems	Approval Signature <i>Julie Ruthven</i>
Who this Policy Applies to All agency employees and contractors	Approval Date 08/06/2008
Number 20.10.1	Scheduled Review Date 08/05/2009

**Purpose** The purpose of this policy is to outline the acceptable use of computer equipment at the Secretary of State (Secretary) to protect the data of the Secretary, and the employee. This includes, but is not limited to, all present and future forms of hardware, software, and services for data processing and office automation.

Information related technology is provided to automate business processes used within the agency, and shall be reserved for the agency's business, with minor exceptions as noted.

**Background** This policy is intended to clarify the acceptable use of information resources and information technology systems. Enforcement of this policy is consistent with the policies and procedures of this organization.

The intent of this policy is to protect the Secretary's employees, and the public customers from illegal or damaging actions by individuals, either knowingly or unknowingly.

**Policies Referenced**  
Asset Classification Policy  
User Password Policy  
Purchasing Policy

---

## Definitions

Term	Definition
Asset	Anything that has value to the agency.
Chain Letter	A message that requests the recipient to write or forward the same or similar email to further recipients.

- Focused on Security. Dedicated to Success. -



# Acceptable Use of Electronic Systems Policy

Client Software for Internet Music	Software that is downloaded and installed to access an internet radio application. Examples: AOL Radio, Napster.
Encryption	Use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.
Junk Mail	Unsolicited advertising material.
Non-Licensed Free Software	Software available on the internet for download and installation on a computer that does not require the purchase of a license.
Unauthorized Equipment	A device that attaches to a computer that has not been approved by the Division Director.

## Policy

### **Ownership of Information Systems and Data**

All systems and information are, and shall remain, the property of the Secretary, and subject to its sole control. No parts of the Secretary's systems or information are, or shall become, the private property of any system user. The Secretary owns all legal rights to control, transfer, or use of all or any part of its systems.

### **Control and Access**

The Secretary can and may trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish, or disclose any information, in accordance with applicable disclosure of information policies. Employees shall have no expectation of privacy, and their activity may be monitored.

Users must not attempt to access documents, files or portions of operating systems, security systems, or administrative systems to which they have no specific business reason to access. Accordingly, users must not access, without specific business reasons, electronic mail, data, programs, or information protected under state and federal laws.

### **Public Records Retention**

All users must comply with public record retention laws and rules. The agency may disclose any public record without permission or knowledge of any system user. Except as noted, users shall not expect that any personal use of the Secretary's systems will be private or privately owned.

- Focused on Security. Dedicated to Success. -



# Acceptable Use of Electronic Systems Policy

## **Passwords**

Users must not use automated password savers. Additional information can be found on the User Password Policy.

## **Web Use**

All use of web technologies shall comply with the Secretary's security policies, and other agency policies, procedures, and guidelines.

All published web content on the Secretary's web servers shall be restricted to the Secretary's business as defined by agency management. When publishing content to the agency website, the content must follow communication guidelines and standards as established by the Secretary. Users may post or publish queries or comments to user groups as it applies to their business roles. Content and frequency must reflect the agency's interest; not the user's.

Downloads of business related information are acceptable as they apply to the user's business roles. Downloads of non-licensed, free software shall be reviewed by ISD and authorized through Division Management. Software for purchase must be approved through Division Management and ISD, and must conform to the agency's Purchasing Policy.

## **Proper Use of Resources**

Except as allowed by policy, systems may be used only for the business of the agency as defined by the agency. Users shall recognize that computing resources are limited and user activities may have an impact on the entire network.

User must not:

- Misuse email by spreading widely or flooding an individual, group, or system with numerous or large email messages.
- Use streaming video or real time applications such as a stock ticker.
- Install an application for the purpose of listening to internet radio.

Users may use streaming audio, video, or real time applications as it is related to their business role.

Users may use non client installed streaming audio for listening to music. Some streaming internet radio stations require client installed for internet music. These applications shall not be installed.

Users shall not knowingly access material that is inappropriate in an office

- Focused on Security. Dedicated to Success. -



# Acceptable Use of Electronic Systems Policy

environment, consistent with State of Oregon policies.

## **Personal Use**

Personal use of the Secretary's technology systems is permitted on an incidental basis. Agency Management and HRD have sole discretion to determine whether use is personal or business and/or if it is incidental use.

Any personal use:

- Must conform to other agency policies.
- Must take place during rest or meal breaks.
- Must be limited, incidental, and minimal. The use shall not be excessive or a part of a daily plan.
- Must be at virtually no cost to the state.
- Must not include installing, downloading or executing personal software, including no cost, non licensed software.
- Must not include connecting privately owned devices to Secretary's network or devices without management authorization.
- Must not adversely impact the capacity of or cause a security risk to information related technology systems.
- Must not include instant messaging technology for personal communications.
- Must not include playing computer games, whether internet, personal, or those included within approved operating systems.
- Must not be for or on the behalf of any organization or third party without agency approval.
- Must not include publishing personal content to the web including personal web pages, personal postings to internet groups, chat rooms, web pages or list services.
- Must not include soliciting, lobbying, recruiting, selling, or persuading for or against commercial ventures, products, religious or political causes, outside organizations, or the like.
- Must not include creating, sending, or forwarding junk mail or chain letters.
- Must not include activities that result in personal gain (financial or otherwise).
- Must not be for political purposes.

Exceptions:

- Limited web searches for professional research and self-study for professional development.

- Focused on Security. Dedicated to Success. -



# Acceptable Use of Electronic Systems Policy

- Limited web searches for preparing a resume or application for a state job.
- Incidental personal use of e-mail and the internet is permitted outside of breaks.

## **Protecting Information and Shared Resources**

Users must:

- Lock their workstations when their work area is visibly unattended.
- Follow established procedures for protecting files, including managing passwords and using encryption technology.
- Protect the physical and electronic integrity of equipment, networks, software, and accounts on any equipment that is for the Secretary's business in any location.
- Not open email that seems suspicious.
- Not knowingly introduce worms or viruses or other malicious code into any system, or disable protective measures, i.e. antivirus, anti-spyware or firewalls.
- Not send restricted or confidential data over the internet unless using agency approved encryption mechanisms.
- Not connect unauthorized equipment or media to an agency device, which includes: laptops, removable drives, wireless access points, PDAs, and mp3 players that have not received Division Director approval.

## **Failure to Comply**

Failure to comply with this policy may result in disciplinary action up to and including dismissal from state service for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal action also may be taken for violations of applicable regulations and laws.

---

### **Guidelines**

- Users can lock their workstations quickly by pressing the Windows key and the letter L.
- If a user inadvertently accesses inappropriate material, the user should contact his/her management and explain the access immediately.
- All files and folders stored on the All Temp network drive will be deleted after 30 days.

- Focused on Security. Dedicated to Success. -