Ecology Email Security and Use Policies

for

Chehalis Basin Board Voting Members

- Executive Policy 15-01: Prohibiting Private Use of State Resources
- Administrative Policy 16-02: Securing Ecology's Information Technology Resources
  - Attachment A
- Administrative Policy 16-08: Using Mobile Devices for Ecology Business
- Administrative Policy 16-11: Using Electronic Message Systems

By using your Ecology issued email to conduct official Chehalis Basin Board business, Board members agree to Ecology security and use policies.

DEPARTMENT OF ECOLOGY
State of Washington

Chapter 15: Ethics/Use of State Resources

Executive Policy 15-01

Resource Contact:	Human Resources Director	**Established:**	August 27, 1990
Reference:	RCW 42.52 RCW 42.56 WAC 292-110-010 Executive Ethics Board Advisory Opinion 02-02A and FAQs Ecology Policies 15-02, 15-03, 15-04, 2-10, 7-14, 3-05, 14-20, 14-10, 16-10, 16-11, 16-02, 16-07, 16-08 Ecology Procedure 15-04-01 Collective Bargaining Agreement	**Revisions Effective:**	January 12, 2010

Prohibiting Private Use of State Resources

Purpose: To ensure compliance with state law and to describe Ecology's position and requirements regarding the use of state resources.

Application: This policy applies to all employees, both represented and non-represented. Represented employees should refer to the Collective Bargaining Agreement for any provisions that may supersede any portion of this policy.

1. State Funds, Equipment, Supplies, Facilities, and Other Resources Are For State Business Only.

Employees may not use state resources, including any person, money, or property under the employee's official control or direction, or otherwise available, for the private benefit or gain of the employee or any other person.

2. Occasional and Limited Personal Use of State Resources is Allowed Under Certain Conditions.

Keeping the general prohibition in paragraph 1 above in mind, employees may make occasional, but limited “de minimis” use of certain state resources if each of the following conditions is met:

A. There is little or no cost to the state.

B. The use of state resources does not interfere with the performance of any officer's or employee's official duties.

C. Any use occurs infrequently.

D. Any use is brief.

E. The use does not compromise the security or integrity of state property, information, software, or the agency’s public image.

See the Collective Bargaining Agreement for specific information about occasional and limited use for union activities.

3. Resources That May be Used Subject to the De Minimis Use Standards Defined in This Policy.

A. Ecology telephones (except cell phones), voice-mail, e-mail, Internet, copy and fax machines, audio-visual equipment, and facilities are all subject to the de minimis standard.

B. Personal visits including family, friends, and children must be limited to break and lunch periods and should be conducted outside the employees work area. These visits must not disrupt others' work, and all Ecology policies regarding visitors to the building must be followed.

C. Storing non-copyrighted personal or non-business related information or material (files, pictures, etc.) on Ecology servers (network) or Ecology computers.

Stored personal material, as well as e-mail and Internet use, is not considered private and is accessible to Ecology, outside regulatory and law enforcement agencies, and through the Public Records Act and legal discovery.

4. Personal Use of Certain State Resources is Strictly Prohibited

A. SCAN authorization codes are for official business only. The only exception is a brief call home when away from home on Ecology business.

B. State-owned cell phones or personal digital assistants are for official Ecology business only due to IRS regulations governing taxable employee benefits.

C. State vehicles are for official business only. Employees may only transport people who are on official state business, and pets are not allowed in state vehicles (see Policy 11-36).

D. Consumable office supplies, such as paper, envelopes, or spare parts, are for business use only; even if the actual cost to the state is minimal.

5. Personal Use of State Resources is Strictly Prohibited for Certain Activities.

Prohibited uses include the following:

A. Promoting, conducting, or participating in an outside business or commercial enterprise of any kind.

B. Supporting, promoting, or soliciting for an outside organization or group, unless allowed by law and authorized by Ecology's director or designee.

C. Using state resources for any personal political use, including campaigning and lobbying for any person, party, or ballot initiative.

D. Using state resources to advertise, shop or browse for, buy, or sell goods or services for private benefit or gain. This includes using Internet-based auction or classified advertising Web sites for advertising, bidding on, buying, or selling personal or commercial goods and services.

E. Accessing, downloading, or disseminating any information that a reasonable person would consider inappropriate for the workplace, such as sexual, violent, or racist material.

F. Accessing or using state information for any personal use unrelated to official business.

G. Installing, downloading, and using unauthorized computer software or games.

H. Sending or receiving personal physical mail to or from the work location or station. Employees may not use any Ecology location as a "ship to" address for personal mail or deliveries.

I. Using Ecology e-mail or logon ID in or on any non-work related Web site.

J. Downloading or storing material that violates copyright or digital rights management law, such as music, videos, or photos.

K. Using agency distribution lists to send e-mail that is not directly related to the employee's job responsibilities.

L. Accessing networks, chat rooms, or bulletin boards for personal, non-agency related purposes.

M. Accessing and using personal blogs or social networking sites such as "MySpace," "Facebook," "Linkedin," or any dating sites, for personal, non-agency-related purposes.

N. Using a state computer to do any sort of personal banking or other financial transactions. The exceptions are transactions related to state-sponsored retirement or benefit programs at Washington State agency Web sites, including making occasional changes to state deferred compensation plan account allocations at the Department of Retirement Systems and to select among health care benefit options from the Health Care Authority.

O. Promoting, conducting, or participating in gambling.

P. Any illegal activity.

6. Personal Internet Activity Requiring Excessive Bandwidth is Prohibited.

There are some activities that use excessive bandwidth (streaming audio or video) and could compromise Ecology network and business activities. Consequently, employees may not stream audio and/or video not related to official job duties, or conduct or participate in any other non-business activity that requires excessive bandwidth - even if the use is brief in duration or infrequent.

7. Fund-Raising for Charitable Organizations is Authorized by the Director in Some Circumstances.

Keeping the criteria in paragraphs 1 and 2 of this policy in mind, employees may participate in fund-raising activities in a state-owned or leased facility, subject to all the following conditions:

A. The activity is in the interest of a legally recognized, bona fide charitable organization.

B. The employee is not directly soliciting co-workers face to face to support or donate to the charitable organization.

C. The employee conducts the charitable work on his/her own time, such as during rest and meal periods.

D. Participation in the activities does not interfere with state business.

E. Employees must comply with any health laws and regulations related to selling food items.

F. The use of state resources is de minimis as described in paragraph 2 of this policy.

G. The activity has been authorized by the Director or designee. Form ECY 010-80 must be completed and submitted for approval, The Director or designee may include specific limitations on the use of state resources for the proposed charitable activity.

H. Managers and supervisors should always refrain from conducting direct, personal solicitations of employees who work under their supervision.

8. The Director May Authorize Limited Personal Use of State Resources For Certain Agency Purposes.

The Director may authorize limited personal use of state resources to promote organizational effectiveness or to enhance the job-related skills of a state officer or employee.

9. Attachment A to This Policy Lists Situational Examples of Authorized and Unauthorized Uses of State Resources.

10. Employee Use of Agency Resources May be Logged and Monitored.

Ecology has the right to log and monitor employee use of agency resources. This includes, but is not limited to, Ecology:

- Computers
- Internet
- E-mail
- Fax
- SCAN
- Cell phones
- Personal Digital Assistants (PDAs)
- Corporate Account (VISA, etc.)
- State vehicles
- Facilities

11. Violating This Policy May Result in Disciplinary Action.

Approved:

Ted Sturdevant
Director

Return to Table of Contents

Chapter 16: Information Technology

Administrative Policy 16-02

Resource Contact: IT Security Officer

Established: March 2, 2000

References: Ecology's Information Security Web Site
Policy 15-01
Policy 16-05
Office of the Chief Information Officer (OCIO) Policy 141
OCIO " Media Handling and Data Disposal Best Practices"

Revisions Effective: June 11, 2014

Securing Ecology's Information Technology Resources

Purpose: To ensure security of and access to Ecology's data and information technology (IT) assets, consistent with Office of the Chief Information Officer (OCIO) standards and all applicable federal and state requirements.

Application: This policy applies to all Ecology employees, represented and non-represented; contractors; employees of tenant organizations; other users of computer systems and network resources supported or owned by Ecology; and to all staff who provide for use, operation, maintenance, and support of those systems. Represented Ecology employees shall refer to the Collective Bargaining Agreement provisions that may supersede any portion of this policy.

1. Establishing Definitions.

Access Exceeding Authority – Accessing IT resources of any type (physical or data) to a degree beyond what is authorized. Example: A user with authority to access data on a specific server circumvents security to obtain access to data that he or she *is not authorized* to view.

Chief Information Officer (CIO) – The person responsible for managing Ecology's central IT resources.

Computer System –Technology comprised of data, applications, software, and hardware that perform a function. Examples: Desktops, laptops, tablets, smartphones or other computing devices.

Computer System User – Any Ecology employee, contractor, employee of tenant organization, or others who use computer systems and/or network resources that Ecology supports or owns.

Ecology Network – All computer systems or devices that access Ecology data or information resources and Ecology's network infrastructure over which that access takes place.

IT Security Officer – The person designated in writing by Ecology's CIO to manage Ecology's IT Security Program.

Information Technology Services Office (ITSO) – The organization within Ecology that provides the agency's central IT functions.

Office of the Chief Information Officer (OCIO) – The OCIO's role in state government is to create clarity and alignment for IT investments. The OCIO security policy can be found at: http://ofm.wa.gov/ocio/policies/manual.asp#security.

Logon ID – The combination of letters, numbers, and/or special characters (such as punctuation marks) a user enters into a computer to identify the user for access to network resources. A logon ID is used with a password and/or another authentication mechanism, such as a smart card, PIN, or biometric identifier (such as a fingerprint). Logon ID may be referred to as Logon Name, Login Name, User ID, or User Name.

Network Access Point – Any point – such as a wireless access point, network jack, or modem – where a device can connect to the Ecology network.

System Administrator – The person responsible for supporting one or more business technology functions. Such support may include hardware or software installation and maintenance, data maintenance, technology monitoring, user roles, and permissions assignments.

Principle of Least Privilege – Least privilege ensures staff access to the data they need to perform their job and restricts their access to all other data.

2. Ecology Provides Security for and Access to Agency Data.

- Security for Ecology's technology is built around protecting confidentiality, integrity, and availability of data.
- Ecology's computer systems are hardened against unauthorized disclosure, alterations, or destruction of data.
- Ecology applies the "Principle of Least Privilege" for accessing agency data. Ecology reduces the risk associated with the unauthorized access or disclosure of agency data by following state level data disposal policies, best practices, and procedures.
- Ecology employees access and process agency data according to Ecology's Data Classification guidelines.
- Public access to Ecology's data is consistent with state of Washington public disclosure laws, rules, and policies.
- Ecology may monitor/audit compliance with this policy.

3. Certain IT Related Activities are Prohibited.

Ecology staff, contractors, vendors, and employees of tenant organizations are explicitly forbidden from engaging in the following activities:

- Allowing vendors, consultants, non-Ecology staff, or other unauthorized people to audit or access the Ecology network or any attached device.
- Hosting Ecology applications and Ecology data outside of the agency network without authorization from Ecology ITSO.
- Adding or using any hardware or software on a computer system that accesses Ecology's network that:

  - Compromises, discloses, alters, destroys, or impedes a computer system or Ecology network security.
  - Compromises, discloses, alters, destroys, or impedes a security investigation.
- Adding an unauthorized device to the Ecology network.
- Altering or disconnecting an authorized device on the Ecology network.
- Introducing unauthorized network communication protocols or technologies to Ecology's network.
- Creating or maintaining a separate network connected to the Ecology network, regardless of purpose, without approval of ITSO.
- Physically accessing the telecommunications closets, computer rooms, or other restricted areas housing Ecology IT resources without authorization.
- Accessing computer system or the Ecology network without authorization.
- Storing Ecology or other business necessary passwords in a location that is not kept confidential (e.g., leaving a password where it could be viewed by others).
- Sharing Ecology or other business necessary passwords.

4. Attachment A Establishes Individual and Group Roles and Responsibilities.

Attachment A to this policy establishes roles and responsibilities for the following people and groups:

- Ecology computer system users.
- Users accessing Ecology systems remotely.
- Ecology system administrators.
- IT Security Officer.
- Vendors, consultants, and other non-Ecology people.

5. Violating This Policy May Result in Corrective and/or Disciplinary Action.

Violating this policy may result in loss of access to Ecology's computer systems or the Ecology network or other corrective or disciplinary action.

Approved: D Stewart

Debbie Stewart
Chief Information Officer

Return to Table of Contents

Attachment A - Policy 16-02

Securing Ecology's Information Technology Resources

This document describes responsibilities of the following types of users:

1. Ecology computer system users.

2. Users accessing Ecology systems remotely.

3. Ecology system administrators.

4. IT Security Officer.

5. Vendors, consultants, and other non-Ecology people.

Everyone is required to comply with the responsibilities listed in all categories applicable to them.

1. Ecology Computer System User Responsibilities.

A. To protect computer systems and data, users:

1) Physically secure all computers and devices taken outside of Ecology buildings.

2) Use Ecology standards to determine the data classification level and appropriate handling of all data used in work duties.

3) Protect data from unauthorized viewing or disclosure.

4) Lock, log off, or power off computer systems when unattended.

5) Ensure computer anti-virus software is enabled.

6) Acquire, install, or run ***no*** software or applications on Ecology workstations, regardless of source, without express approval of the Information Technology Services Office (ITSO). The request for approval should be routed through the IT Help Desk.

7) Host no Ecology applications and data outside of the Ecology network without approval from the ITSO.

8) Install ***no*** hardware on Ecology workstations, regardless of source, without express approval of ITSO.

9) Install ***no*** hardware or software to an Ecology server without authorization from the system administrator or designee.

10) Ensure applications and databases they develop protect Ecology data to the degree appropriate to its sensitivity, and according to the Office of the Chief Information Officer (OCIO) policy and this policy.

11) Dispose of all floppy disks, CDs, and DVDs in Ecology provided media disposal containers.

B. To protect logon identities (Logon ID and password), users:

1) Use only the Logon ID(s) specifically assigned to them.

2) Never share a domain (network) password with any person except an Ecology computer technician performing Ecology duties. Sharing a password with a technician in such circumstances is allowed but not required. (This does not apply to service accounts created by IT staff.)

3) Change each password as soon as possible after it has been shared with a technician or if the password may have been compromised.

4) Never store or display passwords where they may be viewed by others.

5) Never place an unencrypted password in a batch file or other document on any computer system. (This does not apply to system administrators when an unencrypted password is required for proper function of a system they are responsible for.)

C. Users create passwords that meet the following criteria:

1) Passwords must be at least eight characters long.

2) Passwords must contain at least one special character (such as &, =, or an extended ASCII set character) and two of the following three types of characters: upper case, lower case, numeric.

3) Passwords may not contain three or more consecutive characters from the user's Logon ID or full name.

4) Passwords must not consist of a single complete dictionary word, but may include a passphrase.

5) Passwords must be significantly different from the previous four passwords.

Exception: In the case of a particular system not allowing compliance with these criteria, the system administrator will provide a system specific password standard.

D. Users report system access attempts by unauthorized people, violations of this policy, and thefts, as follows:

1) During normal business hours (8-5, M-F):

a) Lacey Building – report to Ecology IT Help Desk.

b) Regional/remote offices - report to local IT staff or Ecology IT Help Desk.

2) During non-business hours:

a) All offices – call Lacey building security guard (360-407-6898).

2. Responsibilities of Users Accessing Ecology IT Resources Remotely.

Users accessing Ecology's network remotely, for example through Virtual Private Networking (VPN), are responsible for:

A. Not caching passwords used for Ecology's network. Checking a dialog box that offers to save or remember a password is an example of caching.

B. Not connecting to any other network, including a home network or an Internet Service Provider (ISP), while connected to Ecology's network, **except** to access Ecology's network using VPN.

C. Ensuring no one else (including family members) has access to a computer that is logged onto Ecology's network.

D. Ensuring confidentiality of Logon IDs, passwords, and other information related to accessing Ecology's network.

E. Using current anti-virus software and signature files on the remote computer.

3. Ecology System Administrator Responsibilities.

Each program/office appoints a System Administrator for each of its applications, servers, and devices hosting server functions covered by this policy. System Administrators are responsible for:

A. Educating and communicating with users to promote a secure environment for their computer system(s).

B. Operating and maintaining their computer systems(s) according to Ecology policies, OCIO Policy 140, 141, 141.10, and Ecology system security procedures, standards, and best practices.

C. Ensuring their computer systems are not running unnecessary or inappropriate services that might negatively impact network stability and/or security. This includes, but is not limited to

1) Domain controllers for unauthorized domains.

2) Domain Name Service (DNS).

3) Windows Internet Naming Service (WINS).

4) Dynamic Host Configuration Protocol (DHCP).

5) Any other services intended to provide functionality that should only be provided at the agency or enterprise level.

D. Coordinating with ITSO on the following:

1) Configuring all operating systems, utilities, and applications for their system(s) to comply with security standards.

2) Ensuring their systems protect Ecology assets to the degree appropriate to their sensitivity.

E. Coordinating with the IT Security Officer for:

1) Defensive actions, reporting, and corrective actions related to system security exposures, attacks, and breaches, including virus infections.

2) Assisting with security audits.

F. Protecting systems and service account passwords by:

1) Meeting or exceeding the requirements for authentication in OCIO Policy No. 141.1.

2) Sharing service account passwords with as few people as feasible.

3) Protecting service account passwords from disclosure to non-authorized personnel.

4) Logging on with a service account password only when absolutely necessary.

5) Storing passwords in clear text **only if** dictated by business needs. It is the System Administrator's responsibility to secure files containing unencrypted authentication information.

4. Ecology IT Security Officer Responsibilities.

The IT Security Officer is responsible for managing the IT Security Program and protecting Ecology's IT resources.

A. The IT Security Officer has the authority to:

1) Monitor and enforce security rules and procedures as directed by OCIO standards and this policy.

2) Disconnect, examine, and/or take possession of any Ecology computer system or component for IT security purposes.

3) Share information with IT security representatives of other state agencies to protect state resources.

B. The IT Security Officer's responsibilities include, but are not limited to:

1) Ensuring this policy is consistent with all applicable laws, regulations, and OCIO policies and standards.

2) Delegating staff to:

a) Monitor for compliance with this policy.

b) Monitor for breaches in network security and take appropriate countermeasures.

3) Providing appropriate follow-up to identified IT security problems and reporting their status to Ecology's CIO.

4) Ensuring a firewall and/or other appropriate protective measures are in place where Ecology is a tenant agency and shares infrastructure with another organization.

5) Establishing effective communications with the appropriate representatives of tenant agencies and ensuring those agencies are aware of and comply with Ecology security policies and standards.

6) Ensuring adequate physical protective measures are implemented for all IT computing resources, coordinating with Ecology Facilities staff when necessary.

7) Working with Ecology Human Resources staff to ensure Ecology meets OCIO standards for personnel security (hiring practices, background checks, etc.).

8) Ensuring staff involved in network security are properly trained and have the background to administer IT security functions.

9) Coordinating with others as necessary to develop Ecology standards, procedures, and best practices for IT security.

10) Promoting a secure environment for all Ecology IT resources.

11) Gathering information regarding current and anticipated security risks, identifying vulnerabilities, and disseminating information necessary to mitigate these risks and vulnerabilities.

12) Reviewing and approving changes to Ecology's IT security program.

13) Reviewing exceptions to this policy. Exception requests must be justified in writing and based on a valid business need.

14) Developing and conducting security awareness training for all users.

15) Developing and conducting security program training for management, IT, and IT-related staff.

5. Security Responsibilities Regarding Vendors, Consultants, and Other Non-Ecology Personnel Accessing Ecology's IT Infrastructure/Resources.

When non-Ecology people need access to Ecology IT resources, the Ecology employee(s) coordinating their services must:

A. Ensure an EPIC profile is created.

B. Ensure their program's service coordinator submits a service request through InfoCentre.

C. Submit a Request for Remote Access if VPN is required.

D. Ensure the non-Ecology people are informed of their requirements to review and comply with:

   1) This policy.

   2) Ecology Policy 15-01, Prohibiting Private Use of State Resources.

   3) OCIO Policy No. 140.

E. Ensure a Service Request form is submitted to InfoCentre when an employee or contractor leaves Ecology.

Return to Policy 16-02

Return to Table of Contents

Chapter 16: Information Technology

Administrative Policy 16-08

Resource Contact: Infrastructure & Operations Manager

Established: July 17, 2003

References: Ecology Policies 15-01, 16-02, and 16-07
State Cellular Device Policy 191

Revisions Effective: October 29, 2015

Using Mobile Devices for Ecology Business

Purpose: To 1) recognize that proper use of mobile devices can promote Ecology's organizational effectiveness; 2) establish protocol for requesting and using these devices; and 3) manage the information transmitted and received with them.

Application: This policy applies to all Ecology employees, represented and non-represented. Represented employees shall refer to the Collective Bargaining Agreement provisions that may supersede any portion of this policy.

1. Establishing Definitions

Ecology Owned Mobile Device – Any mobile device paid for and provided by Ecology to the employee for business use.

Employee – Represented and non-represented Ecology employees, supervisors, and managers; and consultants, contractors, and temporary service employees working for Ecology.

Mobile Device – Any device capable of using the services provided by public or private networks. This includes:

- Pagers
- Cell phones
- Smartphones
- Tablets (includes IPads)
- Laptop computers

Personal Mobile Device – Any mobile device paid for by the employee for personal use.

2. Information Technology Services Office (ITSO) Selects Appropriate Device, Voice, and Data Plans.

The ITSO reviews mobile device options, voice and data plans, and selects the most appropriate, secure, and cost-effective solutions for Ecology to purchase. Mobile devices may only be purchased from this list.

3. Employees May Not Use a Personal Mobile Device to Conduct Ecology Business.

To ensure the security and integrity of the state's resources, and to protect employees' personal devices from potential public disclosure requests, data wipes and litigation holds, employees may not use personal mobile devices to conduct Ecology business.

4. Mobile Device Purchases are Approved According to the Signature and Authority Matrix.

Ecology owned mobile device purchases are approved according to Ecology purchasing processes and Policy 17-01, Attachment A – Signature and Authority Matrix. (See Plan Costs for up to date costs).

Device updates will occur automatically as appropriate and available, unless there is an additional cost for the update. Update costs require the same approval as the original purchase.

5. Information on Mobile Devices is Considered a State Resource.

To ensure appropriate use of resources, including compliance with public records and records retention laws and rules, Ecology has the right to access, inspect, and/or monitor any state resource.

- Any information on the device is subject to monitoring and data capture and is not subject to any expectation of privacy.
- All call records, documents and data, photos, etc. used to conduct state business are subject to records retention requirements and public records laws, rules, and policies.
- Call records and other information (e.g. data, photos, and text messages) may be subject to review or audit in the event of a litigation hold or public records request.
- In some situations, a mobile device accessing state Shared Services may have its data wiped. Some examples of when this might be necessary include:
    - The device is suspected of being compromised and poses a threat to the state.
    - An employee violates State Policy 191 and related statutes concerning the use of an Ecology device.
    - A technical issue arises that requires a device be wiped to resolve.
    - The email or domain account associated with an employee device is disabled.

6. Employees Notify the Ecology IT Help Desk As Soon As Possible if a Mobile Device is Lost or Stolen.

If an Ecology owned mobile device is lost or stolen, the employee notifies Ecology via the Help Desk as soon as possible, but no later than 24 hours from losing the device. This can be done by emailing ecyreishelpdesk@ecy.wa.gov or by calling (360) 407-6911. Once notified, Ecology ITSO staff will confirm the data wipe of the mobile device.

The employee's Ecology network log in will also be reset immediately, and Help Desk staff will generate a new temporary password for the employee's network log in.

Approved: ______________________________

Debbie Stewart
Chief Information Officer

Return to Table of Contents

Chapter 16: Information Technology

Administrative Policy 16-11

Resource Contact: Chief Information Officer

Established: February 23, 1994

References: Executive Order 91-10 (Establishing the Governor's Policy on Electronic Message Systems)
Chapter 42.56 RCW (Public Records Act)
Chapter 40.14 RCW (Preservation and Destruction of Public Records)
Policy 15-01: Prohibiting Private Use of State Resources
Policy 16-07: Preventing Computer Software Piracy
Policy 20-13: Responding to Requests for Ecology Records

Revisions Effective: February 23, 2016

Using Electronic Message Systems

Purpose: To define how Ecology electronic message systems may be used, and explain Ecology's rights to access information sent, received, or stored using state-owned electronic message systems.

Application: This policy applies to all Ecology employees, represented and non-represented. Represented employees shall refer to the Collective Bargaining Agreement for provisions superseding any portion of this policy.

1. Defining Electronic Message Systems.

Electronic message systems include electronic mail, instant messaging (IM), and text messaging systems that store and/or transmit typed communication; voice mail systems that store and/or transmit voice recordings; IM presence; video transmission and storage; facsimile and imaging equipment that store and/or transmit images; and all similar systems.

2. State-Provided Electronic Message Systems May Be Used Only For State Business.

All state-provided information technology resources, including electronic message systems, are the property of the state of Washington and may be used only for state business purposes. See Ecology Policy 15-01, Prohibiting Private Use of State Resources, for specific details about limited personal use of electronic message systems.

3. State-Provided Electronic Message Systems May Not Be Used For Illegal Purposes.

Prohibited uses include:

A. Promoting, conducting, or participating in an outside business or commercial enterprise of any kind.

B. Supporting, promoting, or soliciting for an outside organization or group, unless allowed by law and authorized by Ecology's director or designee.

C. Any personal political use, including campaigning and lobbying for any person, party, or ballot initiative.

D. Advertising, buying, or selling goods or services for private benefit or gain.

E. Conducting personal business beyond de minimis use, as outlined in Policy 15-01.

4. Electronic Message Systems Are Not Confidential.

Electronic messages may be forwarded to others by a recipient, printed in a location where people other than the intended recipient may view messages, or directed to the wrong recipient.

Electronic messages cannot be protected from unauthorized access caused by a user who fails to maintain password security or a user who leaves a device logged onto the system while unattended.

5. Ecology Attempts to Provide Electronic Message Systems That Provide Data Integrity and Confidentiality.

Public records contained on electronic message systems must be maintained according to retention schedules approved by the appropriate records committee according to Chapter 40.14 RCW.

While all electronic messages may be considered writings, and all writings may be public records, certain records are exempt from public disclosure. Chapter 42.56 RCW exempts broad categories of records, and other statutes provide confidentiality of specific records. Ecology maintains sole discretion in applying statutory exemptions and whether records will be withheld from public inspection or copying.

6. Employees Should Not Expect Electronic Messages to be Private.

When using a state-owned electronic messaging system, there should be no expectation of privacy. Records created by these systems may be requested by anyone under the Public Records Act and may need to be produced in "discovery" or during the litigation process. Public records staff who review these records only redact or withhold information specifically exempt by law and do not use a personal privacy standard to determine what is not provided to requestors.

7. Authorized Ecology Staff Have Access to Data.

As authorized by Ecology policy or by the Director or designee, any portion of a user's electronic messaging system may be accessed without consent of the sender or recipient. This may be done as needed to carry out Ecology business functions, in the course of an audit, or if there is reason to believe misuse has occurred. Ecology managers have authority to monitor employee use of electronic messaging systems. Records obtained without the consent of the sender or recipient may be used as the basis for disciplinary action.

8. Records on a Personal Device Are Subject to Access if That Device is Used to Access Ecology's Network Through a VPN Connection Without Approval.

If an employee uses personally-owned systems or devices to do Ecology work without approved remote access to Ecology's network through a VPN connection (see policy 16-07), records on that personal device are then also subject to access. Access to the state mobile e-mail system (Outlook Web APP) is an approved remote access method for e-mail and can be used on personally owned devices.

Approved: D Stewart

Debbie Stewart
Chief Information Officer

Return to Table of Contents