



DEPARTMENT OF CORRECTIONS
Information Systems Services Division



Title:	Electronic Mail, Internet Usage, and Computer Investigations	DOC Policy: 60.1.2
Effective	12/15/08	Supersedes: 10/1/05
Applicability:	All functional units	
Directives Cross-Reference:		
Rules:	Release of Public Record – Div 037 Release of Public Information – Div 039	
Policy:	Criminal Evidence Handling – 70.1.3	
Attachment:	Attachment 1 – Archiving E-mail	

I. PURPOSE

The purpose of this policy is to establish guidelines for the proper use of electronic mail and the Internet and to ensure that all Department electronic information systems are used only for Department business with minor exceptions.

II. DEFINITIONS

A. Department System or Systems: All electronic information devices, interconnections, and technical information of the Department. Examples of systems include:

1. Computers, printers, copiers, recorders, transmitters, data tele-communications connections and any similar connected devices.
2. CIS, ISIS, Outlook e-mail or any other systems accessed by or through these systems or systems devices, such as Internet, external e-mail, and cable television.
3. Designs, specifications, passwords, access codes, encryption codes, and any identifier for devices, users, or accounts.
4. Any published document intended for the public must comply with the DOC rule on **Release of Public Information** (OAR 291-039).
5. All Departmental web sites and web pages must be hosted on an approved internet service provider (ISP).
6. All devices such as cell phones, smart phones, PDAs, MP3 players, USB drives, memory chips and any other portable devices.

B. Information: Information of any kind used in any way in Department systems. Examples include messages, communications, e-mails, files, records, recordings, images, graphics, pictures, photographs, transmissions, signals, programs, macros, software, text and data.

1. Unsolicited messages or data originating from non-DOC systems and personnel and received through Department messaging systems, including e-mail systems are not included in this definition, unless saved through user action, or allowed to remain on local or other system storage devices due to user failure to delete them, once identified. Messages or data, regardless of origin, attached to or included in whole or in part into messages or documents created, saved, or forwarded on DOC systems is included in this definition.
 2. The Department does not express any right to regulate information residing on non-DOC systems not under the Department's management responsibility, control, or jurisdiction.
- C. Publishing: Using systems to disseminate or spread information to the public or beyond the user's area of authority within the Department. Examples include newsletters, web pages, flyers, chain letters, pictures, and posting to Internet groups or to e-mail lists.
- D. Use: Any use of Department systems to affect information in any way. Examples include using systems to search, produce, calculate, extract, forward, print, publish, receive, send, transmit, apply, run control, download, upload, record, copy, rename, access, alter, delete, erase, encrypt or store any information.

III. POLICY

- A. **Electronic Mail.** The Department has chosen e-mail as one of its prime methods of communication to derive the benefits of increased efficiency in communications, reduced reliance on paper, and for its ability to protect information assets while protecting Department integrity and employee rights. DOC encourages the use of e-mail for all Department business, but solely for Department business, except as allowed under DOC policies, agreements, or contracts.
1. The e-mail system and mail generated using this system, including backups, are the sole property of DOC and are not the property of any users of the system. There is no guarantee of privacy or confidentiality for e-mail documents; therefore, users of the e-mail system should carefully consider the nature of what they put into e-mail. E-mail documents have the same legal protection under confidentiality laws as documents written on paper but the ability to secure e-mail documents is more complex. The security risk should be understood and precautions taken when e-mailing documents that contain confidential information (e.g. offender, employee or contract information).
 2. All e-mail documents and user accounts are subject to the Public Records Law and the DOC rules on **Release of Public Information** (OAR 291-039) and **Release of Public Record** (OAR 291-037). The Department does not use the e-mail system to archive old e-mail. Backups are maintained, for short intervals, for system recovery only. When a document is deleted, it is permanently deleted from the system in the next backup cycle. Archiving of e-mail is the responsibility of the each individual. Attached is a procedure to follow for archiving of e-mail.
 3. Electronic mail communications are considered public records and retention and disposition of public records is authorized by retention schedules issued by

the Secretary of State Archives Division. Retention responsibility is up to the individual originating the electronic mail or the DOC staff receiving the document from an outside entity. The retention schedule is located in OAR 166, Division 300 (please refer to http://arcweb.sos.state.or.us/rules/OARS_100/OAR_166/166_300.html). Documents containing attached files need to be filed according to their function and content. These records will have the same retention as the records they are filed with.

- B. **Internet Use.** The Department encourages the use of the Internet for business related research and communication. DOC recognizes the Internet as a business tool that provides vast, diverse and unique sources of information. The Internet is available to employees and other approved users to provide a broad, up to date, resource for business information that is inexpensive and easy to access. Some capabilities and features such as streaming video and real time audio that exceed the network capabilities may be restricted or blocked. Any program or service that is determined to produce an excessive load on the network may be filtered or blocked. Except as allowed under DOC policy, agreements, or contracts, Internet use may be only for Department business as defined by DOC.
- C. **ITS Investigations.** ITS will assist in an inquiry or an investigation as requested by a functional unit manager/designee or staff from the Special Investigations Unit. The functional unit manager/designee should consult with either a Human Resources representative, Special Investigations Unit or both before requesting the inquiry or investigation. The requests shall be sent to the ITS Administrator in writing with specific details regarding the scope of the data to be researched. The ITS manager assigned will work with the requestor to respond in an appropriate time frame. Due to the confidential nature of many investigations, ITS management staff will conduct the investigation and provide needed information to the requestor, Human Resources and Special Investigations Unit, as appropriate to the specific investigation.
1. Investigation requests must be specific as to the period of time to review and content requested. ITS will not always be able to capture the information requested due to storage limitations and server back-up capabilities.
 2. In the event of a police investigation, ITS will work with the Special Investigations Division and follow the policy #70.1.3 **Criminal Evidence Handling**.

IV. IMPLEMENTATION

This policy will be adopted immediately without further modification.

Archiving E-Mail

Purpose:

E-mail is a written form of communications that is used to conduct Department of Corrections business, therefore, it is public record (**ORS 192**) covered by state archiving rules and regulations pertaining to the retention of public record. There is no automatic archiving of e-mail, it is the responsibility of each individual to archive e-mail they have created and sent. The purpose of this procedure is to describe what e-mails need to be archived and how. (**OAR 166-300**)

Procedure

Each individual is responsible for archiving e-mail. Only the original e-mail needs to be archived. All the copies made and distributed do not need to be archived, therefore, e-mail sent out or e-mail received from sources external to DOC need to be considered. The following are guides to retention out of OAR 166-300:

1. Eliminate the junk mail

E-mail that is not directly related to corrections business does not need to be archived. Examples: casual conversations among friends, notices of employee events, notices of lost articles, research materials from vendors, education materials, etc.

2. Select the Retention Schedule

E-mail correspondences fall into one of these categories:

a. Administrative

E-mails that concern any of the business areas of the department are to be saved for five years. Examples: personnel issues, inmate specific issues, meeting minutes, duty instructions, changes in operations, e-mail that provides instruction on any DOC operation, etc.

b. General

E-mails, obviously not directly connected to a specific business function or that outlines a specific action related to DOC operation but are part of conducting DOC business, may be filed as correspondences and are to be saved for one year. Examples: meeting requests, meeting agendas, conversations (private or distributed) with other DOC staff about DOC business, conversations with outsiders about DOC business like vendors or suppliers, etc.

3. Archive The E-mail

The following are some possible methods for archiving e-mails but the list is not all-inclusive:

- a. Print the e-mail *and the attachments* to be archived as paper documents and placed in the official file. Attachments include word processing documents, spreadsheets, displays, or other such attachments. The archiving of the e-mail is not complete if the attachment isn't included.
- b. Save the e-mail to disk or CD (attachments are automatically included). Label the completed disk or CD appropriately with the type of material saved, date of the material, and purge date (example: E-mail from 1-1-2003 through 6-30-2003, Purge 6-30-2008). When copying e-mail to a disk, it is probably most efficient to copy both "administrative" and "general" together and retain them all for 5 years. CDs have a large capacity and are inexpensive.

Attachment 1

- c. Save the e-mail to a folder on the PC hard drive (C:). Call the Help Desk, or see your local TSA, if you need assistance setting up or operating folders on the C: hard drive. The hard drive could easily have sufficient space to maintain e-mails for a full year. E-mails will need to be copied to disk, labeled, and stored before the disk space gets full. For most, this could be done annually but could be done anytime to conserve disk space. Remember, the hard drive will require routine backups.