



**DEPARTMENT OF CORRECTIONS
Information Systems**



Title:	Acceptable Use of Electronic Information Systems	DOC Policy: 60.1.1
Effective:	12/15/08	Supersedes: 8/22/00
Applicability: All DOC employees, contractors, and volunteers		
Directives Cross-Reference: Release of Public Information – Div 039		
Attachments: None		

I. PURPOSE

The purpose of this policy is to ensure that all Department electronic information systems are used only for Department business with minor exceptions.

II. DEFINITIONS

- A. Corrections information System (CIS): A computer system that has information about Inmates in prison and on probation, parole and post-prison supervision.
- B. Chronos: That portion of the CIS that permits authorized users the ability to document an inmate's/offender's issues or progress while incarcerated or on probation, parole or post-prison supervision.
- C. 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.
- D. 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.
- E. 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.
- F. 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. Systems and information are Department property.** All systems and information are the property of the Department, subject to its sole discretion. No part of systems or information, regardless of origin, shall be the private property of any system user, excepting as restricted by prior copyright, HIPAA, or Oregon statute. The Department owns all legal rights to control, transfer, or use all or any part or product of its systems. All uses must comply with this policy.
- B. Systems are for Department business.** Except as allowed under this policy, systems shall be used only for the business of the Department. Department systems shall not be used for labor union purposes, except as specified in a collective bargaining agreement or other legally binding directive.
- C. The Department has full access and control of its systems.**
1. Control: The Department reserves all rights relating to information, regardless of origin, stored in Department systems.
 - a. The Department may trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish, or disclose any information, except as restricted by prior copyright, HIPAA, or Oregon statute, at any time without notice. The Department may withdraw permission for any or all personal or business uses of its systems at any time without cause or explanation. No one will be granted access to Department systems without Department authorization.

- b. DOC uses automated processes for screening all data passing across its network for computer viruses, worms, executable files, or unusually large attachments (programs, visual basic scripts, images, etc.) in order to protect the system from computer hacking and degrading systems performance due to overloading network capacity. DOC does not normally screen the body of messages, addressee, addressor, or subject lines for content, but reserves the right to do so at its discretion.

2. Access:

- a. Passwords, scramblers, encryption methods, remailer services, drop-boxes, or identify-stripping may not be used without Department approval, access, and control.
- b. No user may attempt to access, copy, delete, or alter the message of any other user without appropriate authorization.
- c. A Department system may not be used to attempt unauthorized access to any information or system.
- d. Access to any portion of the CIS must be directly related to the employee's current position duties and responsibilities only.
 - (1) An example of acceptable access would include an employee reviewing chrono notes on an inmate in the employee's housing unit or on the employee's caseload.
 - (2) An example of unacceptable access would include an employee looking up their neighbor for personal background purposes.
- e. If there is any question whether access to any portion of the CIS is acceptable, employees shall consult with their supervisors.

D. Information on Department systems should be considered public information. Because DOC controls the entire DOC electronic network as state property, any information stored on that network, regardless of origin, could be considered public information under public records laws. This includes PCs, e-mail, correspondence, etc., except as restricted by prior copyright, HIPAA, or Oregon statute.

- 1. DOC will determine what information is a public record.
- 2. DOC may disclose any public record at any time without permission or knowledge of any systems users.
- 3. Except as noted in this policy, users may not expect that any personal use of Department systems is private.

E. Uses must reflect a Department image.

- 1. Uses of Department systems do not all have to be formal; however, they must be professional.
- 2. Employees are encouraged to review the Department's mission, vision, values,

Oregon Accountability Model, Code of Ethics and Code of Conduct which, taken in their entirety, help form the basis for the Department's image.

F. Uses must be lawful, ethical, and inoffensive. Uses of Department systems must not be false, unlawful, offensive, or disruptive.

1. Professional Conduct: Unless job duty requires it, DOC networks and systems shall not be used to intentionally view, download, store transmit, retrieve any information, communication or material which is:
 - a. Harassing or threatening;
 - b. Obscene, pornographic or sexually explicit;
 - c. Defamatory or makes discriminatory reference to race, age, gender, sexual orientation, religious or political beliefs, national origin, health, or disability; condones to foster hate, bigotry, discrimination or prejudice;
 - d. Untrue or fraudulent;
 - e. Illegal or promotes illegal activities; facilitates internet gaming or gambling; or contains offensive humor.
2. Legal Compliance: Copyrighted, intellectual property rights or licensed information, regardless of origin, will be used only with full legal right to do so
3. Data Integrity: Users shall not knowingly destroy, misrepresent, or otherwise change the data stored in DOC information systems.
4. Operation Efficiency: Operation or use of information assets shall be conducted in a manner that will not impair the availability, reliability or performance.

G. Electronic Publishing: Publishing must be authorized. All publishing shall be restricted to Department business. All publishing shall be approved by the functional unit manager. Employee group events may be internally published with this approval.

1. Many Internet or e-mail groups exist to share useful information. A user may post queries or represent the Department by posting professional comments to useful groups with approval from his/her functional unit manager. Comments must conform to this policy. Content and frequency of posting must reflect the Department's interest, not the user's.
2. Internal publishing of employee group events are considered mixed Department and personal business and must be authorized by the functional unit manager. Examples include charitable drives, retirements, parties, etc.
3. Printers shall normally be used to print one or two original copies of a document. Additional copies will normally be produced using photocopiers or a print shop. Exceptions shall be approved by the functional unit manager. It is Department policy to encourage double-sided printing and copying where appropriate and available.

H. Security

All use shall protect the technology and DOC information from risk, comply with policies, laws, and regulations, and reflect an acceptable image of DOC thus ensuring the confidentiality and availability of information.

I. **Personal Use: Personal use shall be restricted.** The Department often needs people to remain at work despite personal needs and interests. The Department also needs employees to continuously develop their knowledge and skills. For these reasons, certain personal uses shall be allowed. The Department shall have sole discretion to decide whether a use is personal business. Supervisors shall be responsible for monitoring employee's personal use. Any personal use must satisfy the following provisions. Any personal use:

1. Must be at virtually no cost to the Department.
 - a. Examples of allowed personal uses: an occasional e-mail message, photocopying for which the Department is reimbursed, and limited use of a PC.
 - b. Examples of allowed mixed Department and personal uses: printing and photocopying a Department job application, resume, personnel and benefits papers, and necessary material for Department-paid courses of study.
 - c. Examples of personal uses not allowed: copying and printing for which the Department is not reimbursed, any service or fee, and any use resulting in personal financial gain, non-work related subscriptions to Internet services that generate network traffic, etc.
2. Must always be petty or insignificant compared to use for assigned work.
3. May not be made by, or on behalf of any organization or third party, except professional association work authorized by the functional unit manager.
4. Must not include publishing if the content or purpose is personal. Personal web pages, photos, graphics, images, personal postings to Internet groups, chat rooms, web pages, or list services are prohibited.
5. Must not include personal solicitation. Systems may not be used to lobby, solicit, recruit, sell, or persuade for or against commercial ventures, products, religious or political causes, outside organizations, or the like, except professional association work authorized by the functional unit manager.
6. Must not include the use of any system device that the user does not employ in his or her assigned work. No privately owned device may be connected to a Department system without authorization from ITS. Systems devices taken home shall remain subject to this policy.
7. Must be limited use of the employee's assigned PCs, software, and Internet access. Examples include web searches for personal research, self-study, and preparing a resume or application for a Department job. Personal use must be

done during meal and rest breaks, or before or after work.

8. That creates public folders is subject to approval by the functional unit manager, for the purpose of posting personal items and information like those allowed on an employee bulletin board. Items posted in these public folders are automatically deleted at the expiration of a pre-determined period, normally 30 days. This is an officially sanctioned personal use of Department resources, so long as all applicable Department policies are otherwise adhered to.
9. Must not include installing, downloading, or executing personal software. This includes not-cost, non-licensed software.
 - a. Unacceptable example: User-supplied or Web downloads of screen saver software are not allowed. Only the screen saver software supplied with the operating system of the desktop is allowed.
 - b. Acceptable example: Minimal, limited quantity of personal files placed on the local hard drive only, not on network drives. Files must comply with all other use and security requirements, i.e. no security risk, non-offensive, non-interfering with others or desktop operation.

J. Web Use

1. Use of Web technology: All use of Web technology shall comply with this policy, DOC security policies, and any other DOC policies, procedures, and guidelines relating to the Web.
2. Review of Web content required. All published Web content shall be restricted to DOC business as defined by and through DOC management. All content must be reviewed by a program supervisor or manager prior to publishing. Published content must follow communication guidelines and standards as established by DOC.
3. Posting/publishing on Web: DOC, through supervisors and managers, may authorize a user to post (publish) queries or represent DOC by posting professional comments to useful groups. Comments must conform to this policy. Content and frequency of posting must reflect the interest of DOC, not the user.
4. Ordering goods through Web: Personnel authorized to make payment by credit card for goods ordered through the Web are responsible for the safe and appropriate use of the Internet.
5. Downloads from Web:
 - a. Downloads of business-related information is acceptable.
 - b. Downloads of applications or programs must be authorized by the supervisor and approved by ITS.
 - c. Downloads that would update existing software must be authorized through ITS. Staff shall contact the ITS Help Desk.

6. Establishing new business channels via the Web: DOC Web connections shall not be used to establish new business channels without prior DOC authorization through ITS. Examples include electronic data interchange (EDI) arrangements, electronic malls with on-line transactions, on-line database services, etc.

K. Server Storage for User Created Documents

1. DOC has allocated space on local file servers for user created documents. This space is commonly called the H drive and it looks and acts like a disk drive on the local PC. This H drive space was developed for several reasons:
 - a. The H drive is backed up daily and it is accessible to the owner of the documents from any Department PC.
 - b. Most PCs are now configured to take advantage of the H drive. The Department encourages using H drives for storing documents important to conducting Department business.
2. The server space allocated for the H drives is not unlimited and must be managed. It was never designed for the permanent archiving of documents.
 - a. When documents are no longer needed for immediate usage, they should be removed from the H drive.
 - b. When documents are annual or biennial in nature and are necessary for creating new ones for the next year or biennium, they should be saved to diskettes, CDs, or tape for long-term storage.
 - c. When the allocated space on the file server gets close to filling up, ITS will recommend that all users purge unneeded documents and will work with them to help reduce the overall server space needed for documents.

L. Application Development

1. **Network Applications:** Network applications are defined as any software program designed for multiple users or has a database that is accessed by multiple users and resides on a server attached to any Department system.
 - a. ITS is ultimately responsible for the reliability and security of network applications. Network applications will be developed by or in collaboration with ITS in accordance with ITS standards and practices. Network applications that have not been coordinated through ITS will be removed from service. They will be reinstated after consulting with ITS staff and appropriate standards have been applied.
 - b. Any requests for network-enabled applications are to be submitted to the division IS coordinator.
 - (1) If the division chooses to pursue development of the application, the coordinator will submit a service request to ITS and place a priority on it.

- (2) ITS will work with the coordinator to determine what resources will be used to complete the project. Resources can include ITS staff, ITS contractors, or division staff. Applications done by division staff are required to have an application service agreement signed by the functional unit manager and the IS manager. The form is available in public folders.
- 2. **Stand-alone Applications:** Stand-alone applications will be defined as any software application designed to work on a single PC with a database on that PC or the H drive of the local server.
 - a. Because standalone applications may indirectly impact the operation of the Department system, all standalone applications to be installed on computers connected to the Department system must be approved by ITS.
 - b. The Department encourages the appropriate use of development tools, like Access, to create job efficiency tools for personal use.
 - (1) ITS does not have the resources to support applications developed in this environment so the original developer must support it. The danger in this type of application is the potential that it becomes “mission critical” or, at least, creates a dependency for a business unit. Eventually, the creator of the application will not be available and the application will malfunction leaving the business without support.
 - (2) ITS recommends locations with stand-alone applications have someone document that application so future repairs can be made by any knowledgeable person assigned to fix it.

IV. IMPLEMENTATION

This policy will be adopted immediately without further modification.