	DEPARTMENT OF CORRECTIONS **Information Technology Services**	
Title:	**Acceptable Use of Oregon Department of Corrections Computing Devices and Information**	**DOC Policy: 60.1.1**
Effective:	**8/5/22**	**Supersedes: 1/10/18**
Applicability:	**All DOC Employees, Contractors, and Volunteers that use DOC computing devices, network infrastructure and information housed and maintained both on and off premises.**	
Directives Cross-Reference **Network Information Systems Access and Security—Div 005** **Release of Public Records—Div 037** **Release of Public Information—Div 039** **Acceptable Use of State Information Assets (DAS) – 107-004-110** **Privileged Access to Information Systems (DAS) –107-004-140** **Oregon Information Systems Security Standards** **Public Records Management—10.1.9** **Code of Ethics—20.1.2** **Code of Conduct—20.1.3** **Electronic Mail, Internet Usage and Computer Investigations—60.4.1** **Information Security—60.6.1**		
Attachments:	**None**	

I. PURPOSE

The purpose of this policy is to set acceptable use standards of computing devices, data, and information at the Department of Corrections (DOC).

II. DEFINITIONS

A. Adware: A type of spyware that downloads or displays unwanted ads when a user is online, collects marketing data and other information without the user's knowledge or redirects search requests to certain advertising sites.

B. Department Computing Devices: All electronic information devices, interconnections, and technical information of the department. Examples of systems include, but not limited to:

1. Computers, printers, copiers, recorders, transmitters, data telecommunications connections and any similar connected devices.

2. All portable devices such as cell phones, smart phones, tablets, MP3 players, and any other devices within the department.

3. Networking devices includes routers, switches, VPN concentrators, or any device interconnecting networks.

4. Large scale information systems which provide services to the department such as logon access, file servers, data warehousing, web access, web hosting, mail, and instant message services.

5. Applications such as Corrections Information System (CIS), Integrated Supervision Information Systems (ISIS), DOC 400, or any other systems accessed by or through these systems or systems devices. Methods include, but are not limited to, the Internet, Internet Service Providers (ISP) and DOC hosted connections.

C. Information: Information is computing device data that is put in human readable form to allow analysis, editing, and reproduction in/on department systems. Examples include, but are not limited to:

1. Documents, reports, statistics, files, records, compiled or stored on DOC computing devices or applications.

2. E-mails or messaging system conversations and their attachments.

3. Audio and video files.

4. Images, graphics, pictures, and photographs.

5. Programs (such as CIS, ISIS, WebLEDS, etc.), software, and macros.

6. Text and data.

D. Publishing: Using computing devices to create, edit, and disseminate information for the consumption and use by department employees, contractors, volunteers, third party, and external entities. Some examples include other state agencies and their employees, State of Oregon residents, cloud solution providers, etc.

E. Removable Media: Any storage device that can be portable, accessible, or connected to any computing device with the ability to process the contents held on that media. Examples include, but are not limited to:

1. USB-based memory sticks (Flash or Thumb Drive).

2. Removable memory cards in any format (Secure Digital, Multimedia, and Compact Flash).

3. Portable audio/media players that internally or externally supports data storage.

4. Cell phone handsets, smartphones with internal or hard drive-based memory.

5. Digital cameras with internal or external memory support.

6. Removable memory-based media such as writable or re-writable DVDs, CDs, or floppy disks.

F. Spyware: Software that is installed secretly and gathers information about the user's Internet browsing habits, intercepts the user's personal data, etc., transmitting this information to a third party.

III. Policy

A. DOC Computing Devices or Resources

1. Acceptable Use of DOC Computing Devices or Resources

a. Except as allowed under this policy, all department computing devices shall be used for department business only, unless explicitly defined under this policy.

i. An example of acceptable computing device usage would include an employee reviewing Chrono notes on an inmate in the employee's housing unit or on the employee's caseload.
ii. A privileged user exercising their privileges to maintain DOC network connectivity.

b. Users shall not expect or assume that use of department computing devices is private.

c. Employees, contractors, and volunteers are responsible for exercising good judgment regarding the reasonable usage of DOC computing devices and their capabilities.

d. Web technology may be used in day-to-day operations to conduct department business. Examples of authorized uses of the web by DOC employees are below. Items include, but are not limited to:

i. Posting or publishing professional comments to useful groups as a representative of DOC.
ii. Ordering goods through the web for official DOC purchases.
iii. Downloading of business-related information.
iv. Downloading of applications or programs that are authorized by a supervisor and approved by Information Technology Services (ITS).

2. Unacceptable Use of DOC Computing Devices or Resources

a. Additional passwords, scramblers, encryption methods, remailer services, cloud-based file storage and file transfer programs, or identity and system

resource anonymizers without expressed consent from the department. ITS will maintain access and control of these applications.

b. DOC computing devices may not be used to attempt unauthorized access to any system, internally or externally connected to the department or any other entity, regardless of approved or unapproved credentials. Items include, but are not limited to:

   i. An employee looking up their neighbor in LEDS for personal background purposes.
   ii. An employee creates or uses a non-DOC approved cloud-based storage and file transfer program (i.e., Dropbox) to store department information for ease of access for home use.

c. Connecting personal computing devices, removable media, peripheral items (i.e., printers, scanners, etc.) and installing programs or software on department computing devices or services is strictly prohibited. Items include, but not limited to:

   i. Connecting personally owned computing devices to the department guest wireless network for personal use or gain.
   ii. Connecting a personally owned removable media to department computing devices to upload DOC information.
   iii. Downloading, installing, or launching programs or software such as chat programs, anonymizers, or games for personal use on department computer devices.

d. Users may not use any DOC computing device for purposes that are unlawful, unethical, offensive, or disruptive to the normal operations against DOC Policy 20.1.2, Code of Ethics or DOC Policy 20.1.3, Code of Conduct. DOC employees shall not use department computing devices or resources for the intentional viewing, download, storage, transmission, or retrieval of information, communication, or material that is:

   i. Harassing or threatening.

   ii. Obscene, pornographic, or sexually explicit.

   iii. Defamatory, inflammatory, or discriminatory in reference to race, age, gender, sexual orientation, religious, or political beliefs, national origin, health, or disability; condones to fostering hate, bigotry, discrimination, or prejudice.

e. Manipulate operational efficiency by impairing the availability, reliability, or performance of DOC computing devices or resources. Examples include, but not limited to:

i. Unauthorized, misuse or abuse of privileged accounts.

ii. Excessive Internet usage which has a negative impact on bandwidth inhibiting normal business operations (i.e., excessive audio/video usage).

iii. Visiting websites that could contain malware, viruses, that might be embedded on websites.

iv. Unauthorized Broadcast e-mails (i.e., Spam, "Reply to All").
v. Chain Mail.

f. Storing personally owned items on DOC computing device or resources. Examples include, but are not limited to:

i. Excessive number of photos, images, etc.

ii. Audio/Video files of any type.

iii. Personal or unapproved programs and software.

B. Use, Ownership and Distribution of Department Information

1. Acceptable Use, Ownership, and Distribution of Department Information

a. All DOC employees, contractors and their subsidiaries, volunteers, or third-party information created, modified, downloaded, or stored on computing devices either owned or leased by DOC remains the sole property of the department.

b. Authorized DOC offices will determine what information is releasable to the public.

c. DOC may disclose any public record, at any time, without user's consent or knowledge.

d. Information transmitted either from or to the department, including e-mail communications, both department-owned or personally owned, are subject to potential tracing, interception, audit, inspection, blocking, restricting, recovery, restoration, and publication.

e. Users must protect information at the Information Security level in which it holds through physical and technical means defined in DOC Policy 60.6.1, Information Security.

i. Health Insurance Portability and Accountability Act (HIPAA).

ii. Private Healthcare Information (PHI).

iii. Any communication that contains Personally Identifiable Information (PII).

f. Employees must use department e-mail or approved file transfer processes to send or receive privileged, confidential, or protected information. That information must only be sent to other DOC computing devices or external entities authorized to receive information.

2. Unacceptable Use, Ownership, and Distribution of Department Information

a. Users shall not knowingly destroy, misrepresent, tamper, or change without authorization information stored on department computing devices.

b. Distribution of department information via personal computing devices, removable media, or personally owned e-mail addresses or cloud storage solutions is strictly prohibited.

i. In the event that any department information that has been sent to personally owned computing device, removable media, public e-mail addresses or cloud storage solutions remains the property of DOC.

ii. In the event that any department information has been sent to a personally owned computing devices, removable media, personal e-mail accounts and cloud-based solutions, that information could become discoverable in an investigation or litigation.

c. No user may attempt to access, copy, delete, or alter DOC information without explicit permission from the information owner or ITS Security.

C. Personal use of DOC Computing Devices and Resources

1. Acceptable Personal Use of DOC Computing Devices and Resources

a. Must not impose additional funding burden to department.

b. Must not hinder or disrupt daily work productivity.

c. Brief and infrequent usage of department e-mail. This includes but not limited to:

i. Notifying family members of mandatory overtime.

ii. Emergencies (transfer to hospital after incident, running late, etc.).

2. Unacceptable Personal Use of DOC Computing Devices and Resources

a. Must not publish content that is not related to normal work assignments. This includes but not limited to:

i. Personal web pages or list services not authorized by management.

ii. Photos, graphics, images.

iii. Personal postings to Internet groups or chat rooms.

b. Must not include personal solicitation:

i. Lobbying, recruitment, or persuade for or against:

(1) Commercial ventures

(2) Religious or political causes

(3) Outside organizations

c. Must not include downloading, executing, or installing software; this includes, but not limited to:

i. User-owned or Internet downloaded screen savers due to malware exposure.

ii. No-cost or non-licensed software due to possible spyware and adware installation.

iii. Personally owned software and programs due to licensing violations.

d. Must not redistribute department assets (i.e., computing devices, removable media, etc.) outside normal state excess equipment policies and procedures; this includes, but not limited to:

i. Theft of DOC computing devices, or parts or software for home use or personal gain.

ii. Reproduction and installation of department software or licensing on personal computing devices for home use or personal gain.

D. Personal Use and Distribution of DOC Information

1. Acceptable Personal Use and Distribution of DOC Information

a. Use of department information can be used in accordance with applicable Oregon Revised Statutes (ORS), Oregon Administrative Rules (OAR) and department policies.

2. Unacceptable Personal Use and Distribution of DOC Information

a. At no time will department employees, contractors, third party vendors or volunteers use DOC information for personal use or gain.

Iv. IMPLEMENTATION

This policy will be adopted immediately without further modification.

Certified: __signature on file_____
Julie Vaughn, Rules Coordinator

Approved: __signature on file_____
Heidi Steward, Acting Director