	DEPARTMENT OF CORRECTIONS **Information Technology Services**	
Title:	**Electronic Mail, Business Communication Platforms, Internet Usage and Employee Services and SIU IT Investigation Requests**	**DOC Policy: 60.4.1**
Effective:	**8/5/22**	**Supersedes: Renumbered from policy 60.1.2 dated 1/10/18**
Applicability:	**All DOC Employees, Contractors, and Volunteers**	
Directives Cross-Reference: **Release of Public Records (OAR)—Div 037** **Release of Public Information (OAR)—Div 039** **Acceptable Use of Oregon Department of Corrections Computing Devices and Information—60.1.1**		
Attachments:	**None**	

I. PURPOSE

The purpose of this policy is to set authorized use standards of electronic mail (email), instant messaging (IM), and Internet usage on computing devices at the Department of Corrections.

II. DEFINITIONS

A. Department System or Systems: 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 telecommunication 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.

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

1. Incoming and outgoing email and IM communications, computer logs, attachments in any format, files, records, recordings, images, graphics, pictures, photographs, transmissions, signals, programs, macros, software, text, data, audio, and video.

2. Data allowed to remain on DOC or personal computing devices or removable media. Emails, IM, 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 are included in this definition.

C. Malicious Logic: Hardware, firmware, or software that is intentionally included or installed onto a system to perform an unauthorized action or process that will have a negative impact on the confidentiality, integrity, or availability of DOC computing devices.

D. Publishing: Using systems to distribute 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 email lists.

E. 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. Email Usage: The department mandates that all electronic DOC business, where applicable must be through department email only. Exceptions are dictated through DOC policies and contracts.

1. All emails (both business and personal) sent, received, routed, or stored within DOC computing devices, network infrastructure or locally is considered DOC property.

2. All emails (both business and personal) sent, received, routed, or stored within DOC computing devices, network infrastructure or locally is subject to State of Oregon public information and record statutes, administrative rules, retention schedules, and policies.

3. All emails and documents that are sent outside the department's control and contain the following information must be encrypted. Examples are, but not limited to:

a. Personally Identifiable Information

b. Personal Healthcare Information

c. Financial Information that contains:

(i.) Personally Identifiable Information

(ii.) Account numbers or codes that could be used for fraudulent activity if released.

4. Any retrieval of archived emails or calendars through system recovery must be requested through the Help Desk.

5. It is the responsibility of all DOC employees, contractors, and volunteers to protect department email resources from internal and external threats. Examples of these threats include, but not limited to:

    a. Unsolicited emails from unknown parties

    b. Unrequested or suspicious links

    c. Attachments

B. Business Communications Platform**:** The department provides a Business Communication platform to allow rapid business communication, when made available to users. Exceptions are dictated through DOC policies and contracts.

1. Business Communication Platforms cover a wide variety of platforms. Example of these include, but are not limited to:

    a. Chat software (Skype for Business, WebEx, etc.)

    b. Text messaging

2. All activities (both business and personal) sent, received, routed, stored within DOC computing devices, network infrastructure or locally stored information and conversations are considered DOC property.

3. All activities (both business and personal) sent, received, routed, or stored within DOC computing devices, network infrastructure or locally is subject to State of Oregon public information and record statutes, administrative rules, retention schedules, and policies.

4. All activities and attached documents that are sent and contain the following information must not be sent via this method. Examples are, but not limited to:

    a. Personally Identifiable Information

    b. Personal Healthcare Information

    c. Financial Information

C. Internet Use: The department provides the use of the Internet for business related research and communication, where applicable. Exceptions are dictated through DOC policies and contracts.

1. Internet usage is monitored, captured, and stored for historical usage data, outages, monitoring and reporting purposes.

2. The department understands that there is need for using streaming media and videos. This activity must be limited specifically to the business and operation of the department.

3. DOC employees will not stream videos and real time audio that place an unnecessary load on computing devices or network infrastructure. Continued

excessive use will cause negative impact to all department users. Examples are, but not limited to:

a. Loss of network connectivity

b. Slow responsiveness to Business applications

c. Expose DOC assets to possible malicious logic

4. Transmission of DOC employee, inmate, contractor, or volunteer information via the Internet must be protected by current industry standard encryption. Examples of information are, but not limited to:

a. Personally Identifiable Information

b. Personal Healthcare Information

c. Financial Information

D. Employee Services and SIU IT Investigation Requests: ITS Security will assist in investigative inquiries as requested by functional unit manager, Employee Services, or SIU. It is recommended that the functional unit manager consult Employee Services, SIU, or both prior to making an investigative inquiry request. All requests must be sent to ITS Security via email at dlitssecurityconfidental@doc.state.or.us to initiate the investigative inquiry request for final CIO approval. ITS Security staff will accomplish all requested tasks based on both the request and information available. Once completed, ITS Security staff will notify either Employee Services, SIU, or both and provide the location where the information is stored.

1. All investigative inquires must be as specific as possible; period of time to review and content requested are two examples. ITS may not have all the information requested due to storage limitation or server back-up capabilities.

2. In the event that a Employee Services or SIU investigative inquiry divulges criminal behavior or violation of the law, ITS Security will halt the investigation immediately. ITS Security will work with the Special Investigation Unit and follow policy 70.1.3, Criminal Evidence Handling.

V. 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