INFORMATION SERVICES PROCEDURES FOR ACCESSING EMPLOYEE ELECTRONIC RECORDS

I. INTRODUCTION

The University of Oregon ("University" or "UO") encourages the use of electronic communications and storage to share information and knowledge in support of the University's mission and to conduct the University's business. The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications and records. This Procedure reflects the principles within the context of the University's legal and other obligations, while also seeking to ensure that UO records are accessible for the conduct of the University's business.

Eligibility to access or use the University's electronic communications services or electronic communications and electronic storage resources, when provided, is a privilege accorded at the discretion of the University. Pursuant to the UO's Acceptable Use Policy, the University owns, controls, and has a custodial relationship with respect to its electronic communication and electronic storage systems and certain classes of information stored on those systems, including, for example, email and files containing UO administrative data, communications pertaining to UO business, operations, governance, and deliberative activities, and proprietary information As a general matter, because such information is UO property, employees have no expectation of privacy in such data. Furthermore, such data are subject to the Oregon Public Records Law. However, the University's Acceptable Use Policy does allow for incidental personal use of UO electronic communication systems, and the University therefore adopts the following procedures to respect the privacy of its employees.

This procedure does not apply to the institution and maintenance of a legal hold, which involves only preservation of data, as contrasted with later access to the data for purposes of discovery, investigation, and the like. For more information about legal holds visit https://generalcounsel.uoregon.edu/holds-discovery.

II. GENERAL REQUIREMENTS AND OBLIGATIONS

A. Access with Consent.

As a general matter, the University does not examine or disclose electronic records without the holder's consent. Consent obviates the need to proceed to the process set forth below in II.B. and can simply be documented in this form. Nevertheless, subject to the requirements for authorization, notification, and other applicable conditions specified in this Procedure, the University may examine or disclose electronic records under very limited circumstances as described below.

B. Access Without Consent.

The University shall permit the examination or disclosure of electronic records without the consent of the holder of such records only:

(i) when required by and consistent with state or federal law;

(ii) when there is information that, if true, would violate University expectations, as defined in Section IV, or state or federal law;
(iii) when there are compelling circumstances as defined in Section IV; or
(iv) under time-dependent, legitimate operational circumstances as defined in Section IV.

(*See Section III for Examples of Types of Access.*)

When, under the circumstances described above, electronic records must be examined or disclosed without the holder's consent, the following shall apply:

1. Authorization. Except for subpoenas, search warrants, or discovery in accordance with Section II.B.7 (Search Warrants, Subpoenas, and Discovery) below, such actions must be authorized in advance and in writing by the top-level administrative individual of the college, department, or unit (e.g., Vice Provost/Vice President/Dean/Department Head), after consultation with the Office of the General Counsel. The person approving cannot be the requestor. If the office structure does not have one of these individuals, authorization must be approved directly by the Office of the General Counsel. Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation. The initial request and subsequent approval must be submitted to the Information Security Office using the form located at *https://forms.uoregon.edu/form/launch/electronic-records-access-request*.

2. Access to the Electronic Records: When accessing records for a request, the work needs to be performed as a collaboration between the Technical Staff identified in the request and the Requester, or their designee. The Technical Staff, as the data custodian, will provide access to data within the parameters of the request, while the Requester, or their designee, will evaluate the data as to its validity within the parameters of the request. This collaboration is in place to ensure that only the necessary data within the parameters of the request is accessed.

3. Emergency Circumstances. In emergency circumstances as defined in Section IV, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately by the University, working through the office of Information Services, without authorization, but appropriate authorization must then be sought without delay following the procedures described in Section II.B.1 (Authorization), above. Prior consultation with the Office of General Counsel is urged.

4. Annual Report/Notification. When required by state or federal law or collective bargaining agreement (CBA), the responsible authority noted above shall at the earliest opportunity that is lawful and consistent with other University policies notify the affected individual of the action(s) taken and the reasons for the action(s) taken. The applicable CBA, if any, should be consulted to determine potential notification obligations contained therein. The University will also issue, in a manner consistent with law, an annual report summarizing the number of instances of authorized or emergency nonconsensual access pursuant to the provisions of this Section II.B (Access Without Consent), without revealing personally identifiable information. Specifically, at the beginning of each calendar year, the Information Security Office will prepare a report for the Office of General Counsel, disclosing the number, type and basis of access requests that occurred during the previous calendar year.

5. Compliance with Law. Actions taken under Sections II.B.1 (Authorization) and II.B.3 (Emergency Circumstances) will be in full compliance with the law and applicable University policies. Advice from the Office of the General Counsel must always be sought prior to any action involving electronic records (a) stored on equipment not owned or housed by the University, or (b) whose content is protected under, for example, the federal Family Educational Rights and Privacy Act of 1974, the Health Insurance Portability and Accountability Act and implementing regulations, or University policies pertaining to education records and personal faculty records.

6. Review and Appeal. Applicable grievance procedures under University policies and Collective Bargaining Agreements shall provide for review and appeal of actions taken under Sections II.B.1, Authorization, and II.B.3, Emergency Circumstances to provide a mechanism for recourse to individuals who believe that actions taken by employees or agents of the University were in violation of this Procedure.

7 Search Warrants, Subpoenas and Discovery. Search warrants, subpoenas, and discovery are not subject to sections II.B.1, 3 and 5-6, above. All search warrants, subpoenas, and discovery requests for electronic records shall be referred to the Office of the General Counsel.

Search Warrants. Duly signed search warrants shall be processed in accordance with federal and state laws, University policies, and instructions in the warrant.

Subpoenas. Subpoenas or other court orders shall be processed in accordance with applicable federal and state laws and University policies.

Discovery. Discovery requests shall be processed, and any advance notice to affected individuals will be provided, in accordance with applicable federal and state laws and University policies.

III. EXAMPLES OF ACCESS TO EMPLOYEE ELECTRONIC RECORDS

A. Compelling circumstances or under time-dependent, legitimate operational circumstances.

1. While Current Employee Is on Leave.

If access to an employee's electronic records is requested while the employee is out of the office on leave:

a. Access may be granted only to the extent and for such time as necessary to comply with the request, and access shall be limited to the least perusal of contents and the least action necessary to resolve the situation. After such time, access should be revoked to anyone other than the account owner.
b. The request must be approved by the top-level administrative individual (Vice Provost/Vice President/Dean/Department Head) of the college, department, or unit after consultation with the Office of the General Counsel. If the office structure does

not have one of these individuals, it must be approved directly by the Office of the General Counsel. The person approving cannot be the requestor. If the top-level Administrator is the person initiating the request, it must be approved by their supervisor; if the individual has no supervisor, or if the supervisor is the University President, the request can be approved by the Office of the General Counsel.

c. Notification shall be provided by the responsible authority pursuant to Section II. B.4., above.
d. The designated technical staff will work in collaboration with the requestor (or someone properly authorized) to search for and access the specific information needed, in accordance with paragraph II.B.2 above.

All units are encouraged to work with employees who will be on any type of leave in order to continue the legitimate business/operations of the unit. For example, "out of the office" email messages can be used to let the sender know that the employee is out and can provide guidance on who to contact in the interim.

B. Required by law or upon information that, if true, would violate state or federal law or University expectations.

If access to an employee's electronic records is needed due to a search warrant, subpoena, investigation, legal action or proceeding (excluding legal holds required by state and/or federal law):

1. Access to specific information in the holder's electronic records must be (a) required by law or (b) where there is information that, if true, would violate University expectations (as defined in Section IV), or state or federal law, as defined in Section IV, below.
2. For access under subsection (b), above, the request must be received from or initiated by a unit with the authority to make these requests (e.g., the Office of the General Counsel, UO Police Department, Human Resources, Office of Internal Audit).
3. For access under subsection (b), above, the request must be approved by the top-level administrative individual (Vice Provost/Vice President/Dean/Department Head) of the college, department, or unit after consultation with the Office of the General Counsel. If the office structure does not have one of these individuals, authorization must be approved directly by the Office of the General Counsel.
4. A copy of the retrieved electronic records will be provided to the requestor by the technical staff assigned to fulfil the request and in accordance with paragraph II.B.2 above.
5. Based on the governing law, the employee may or may not be notified. If notification is warranted, it shall be provided by the official responsible pursuant to Section II. B.3., above.

C. Former University Employees.

1. Internal Access Regarding Former Employees.

If internal access to a former or deceased employee's electronic records, if any, is requested:

a. The request should come from the former employee's unit.
b. The request must be approved by the top-level administrative individual (Vice Provost/Vice President/Dean/Department Head) of the former employee's unit after consultation with the Office of the General Counsel. The person approving cannot be the requestor. If the office structure does not have one of these individuals, authorization must be approved directly by the Office of the General Counsel.
c. Live access to any electronic system or account shall not be provided.
d. All University work-related electronic records can be made available to the requestor, in accordance with paragraph II.B.2 above.
e. A good faith effort must be made to ensure that personal electronic records are not made available unless required by law, compelling or emergency circumstances, or when there is information that, if true, would violate University expectations or state or federal law. *See Section IV (Definitions)*.

2. External Access Regarding Former (Deceased/Incapacitated) Employees.

If external access to electronic records of a deceased or incapacitated employee is requested by family members or legally authorized representatives:

a. The request must come from the personal representative/executor of the deceased employee pursuant to a power of attorney, will, applicable intestacy rules, etc.
b. The request will be forwarded to the former employee's unit.
c. The request must be approved by the top-level administrative individual (Vice Provost/Vice President/Dean/Department Head) of the former employee's unit after consultation with the Office of the General Counsel. The person approving cannot be the requestor. If the office structure does not have one of these individuals, authorization must be approved directly by the Office of the General Counsel.
d. Live access to any electronic communications system, electronic storage system or account shall not be provided.
e. All personal electronic records can be made available to the requestor, in accordance with paragraph II.B.2 above.
f. University work-related electronic records shall not be made available.

IV. DEFINITIONS

Compelling Circumstances: Circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, loss of noteworthy evidence of one or more violations of law

or of University policies, or significant liability to the University or to members of the University community.

Electronic Communications: Any transfer of signals, writings, images, sounds, data, or intelligence that is, created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems.

Electronic Communications Records: The contents of electronic communications created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems or services. This definition of electronic communications records applies equally to attachments to such records and transactional information associated with such records (i.e., information, including electronically gathered information, needed either to complete or to identify an electronic communication including but not limited to electronic mail headers, summaries, addresses and addressees; records of telephone calls; and IP (Internet Protocol) address logs).

Electronic Communications Resources: Telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that supports electronic communications services.

Electronic Communications Systems or Services: Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.

Electronic Records: is information recorded by a computer that is produced or received in the initiation, conduct or completion of a University or individual activity. Examples of electronic records include e-mail messages, e-mail headers, word-processed documents, electronic spreadsheets, digital images, databases and other electronic file types and formats. Many electronic records are maintained as part of an electronic record keeping system, such as geographic information systems (GIS), digital image storage systems, computer aided design (CAD) systems, etc. These records can be stored on electronic communication and storage systems on-site or cloud services.

Electronic Storage Resources: Any electronic device or service that can be used to store data. This includes but is not limited to internal and external hard drives, CDs, DVDs, USB drives, on-campus network attached storage and file share infrastructure, as well as off-campus enterprise cloud UO services such as Microsoft OneDrive, Azure, and similar services.

Electronic Storage Systems or Services: Any storage, collaboration, publishing, or distribution system that depends on electronic storage resources to create, edit, share, store copy, download, display. View, read, or print electronic records for the purpose communication across electronic communications

network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic storage or is implicitly used for such purposes.

Emergency Circumstances: Circumstances in which time is of the essence and there is a high probability that delaying action would almost certainly result in compelling circumstances.

Holder of an Electronic Record ("Holder"): A user who, at a given point in time, is in possession (see definition below) or receipt of a particular electronic record, whether or not that user is the original creator or a recipient of the content of the record.

Possession of Electronic Record: An individual is in possession of an electronic record, whether the original record or a copy or modification of the original record, when that individual has effective control over the location of its storage or access to its content. Thus, an electronic record that resides on a server awaiting download to an addressee is deemed, for purposes of this Procedure, to be in the possession of that addressee. Systems administrators and other operators of University electronic communications services are excluded from this definition of possession with regard to electronic records not specifically created by or addressed to them.

- Users are not responsible for electronic records in their possession when they have no knowledge of the existence or contents of such records.

University Expectations: University or unit-level policies or procedures, collective bargaining agreements, and other publicly posted or clearly communicated University procedures or processes.

Time-dependent, Legitimate Operational Circumstances: Circumstances in which failure to act could seriously hamper the ability of the University to function administratively or to meet its teaching obligations but excluding circumstances pertaining to individual personal or professional activities, or to faculty research or matters of shared governance.