INFORMATION SERVICES PROCEDURES FOR ACCESSING EMPLOYEE ELECTRONIC COMMUNICATIONS RECORDS

I. INTRODUCTION

The University of Oregon ("University" or "UO") encourages the use of electronic communications 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. This Procedure reflects the principles within the context of the University’s legal and other obligations, while also seeking to ensure that UO administrative 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 resources, when provided, is a privilege accorded at the discretion of the University. Pursuant to UO’s Acceptable Use Policy, the University owns, controls, and has a custodial relationship with respect to its electronic communication systems and certain classes of information stored on those systems, including, for example, email 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.

II. GENERAL REQUIREMENTS AND OBLIGATIONS

A. Access with Consent.

As a general matter, the University does not examine or disclose electronic communications records without the holder’s consent. Nevertheless, subject to the requirements for authorization, notification, and other conditions specified in this Procedure, the University may examine or disclose electronic communications under very limited circumstances as described below.

B. Access Without Consent.

The University shall permit the examination or disclosure of electronic communications 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 substantiated reason, as defined in Section IV, to believe that violations of law or of University policies have taken place;
(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 communications records must be examined or disclosed without the holder’s consent, the following shall apply:

1. **Authorization**. Except in emergency circumstances (as defined in Section III) in accordance with Section II.B.2 (Emergency Circumstances), below, or except for subpoenas or search warrants in accordance with Section II.B.6 (Search Warrants and Subpoenas), 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 Chief Information Security Officer (ciso@uoregon.edu).

2. **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 if time permits.

3. **Notification and Annual Report**. 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 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.

4. **Compliance with Law**. Actions taken under Sections II.B.1 (Authorization) and II.B.2 (Emergency Circumstances) shall 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 communications records (a) stored on equipment not owned or housed by the University, or (b) whose content is protected under 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.

5. **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.2, 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.
6. Search Warrants and Subpoenas. Search warrants and subpoenas are not subject to sections II.B.1-2 and 4-5, above. All search warrants and subpoenas for electronic communications 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. The University shall provide advance notice to individuals whose records are the subject of a subpoena ducès tecum in accordance with applicable federal and state laws and University policies.

III. EXAMPLES OF ACCESS TO EMPLOYEE ELECTRONIC COMMUNICATIONS 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 communications records are requested while the employee is out of the office on leave:

1. There must be compelling circumstances or time-dependent, legitimate operational circumstances, as defined in Section IV, below, to access specific information in the account holder’s electronic communications records.
2. Such access may be granted only to the extent and for such time that the compelling circumstances or time-dependent, legitimate operational circumstances exist, 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.
3. The request must be approved by the top-level Administrative individual (Vice Provost/Vice President/Dean/Department Head) of the college, department, or unit. 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.
4. The initial request and subsequent approval must be submitted to the Chief Information Security Officer (ciso@uoregon.edu).
5. Notification shall be provided by the responsible authority pursuant to Section II. B.3., above.
6. Someone other than the requestor (but at all times someone properly authorized) should search for and access the specific information needed.

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 a substantiated reason to believe that a violation of law or University policy has taken place.**

If accesses to an employee’s electronic communications records are needed due to a search warrant, subpoena, investigation, legal action or proceeding:

1. Access to specific information in the holder’s electronic communications records must be (a) required by law or (b) upon a substantiated reason to believe that a violation of law or University policy has taken place, 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, and Chief Human Resources Officer).
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 responsive electronic communications record will be provided to the requestor.
5. Based on the governing law, the employee may or may not be notified. If notification is warranted, it shall be provided by the responsible official 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 communication records, if any, is requested:

1. The request should come from the former employee’s unit.
2. 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.
3. The initial request and subsequent approval must be submitted to the Chief Information Security Officer (ciso@uoregon.edu).
4. Live access to any electronic communications system or account shall not be provided.
5. All University work-related electronic communications records can be made available to the requestor.
6. Personal electronic communications records shall not be made available unless required by law, compelling or emergency circumstances, or when a substantiated reason exists that violations of law or University policies have occurred. See Section IV (Definitions).
7. A good faith effort must be made to provide notice to former employees prior to access by the responsible authority pursuant to Section II B.3, above.

2. **External Access Regarding Former (Deceased) Employees.**

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

1. The request must come from the personal representative/executor of the deceased employee pursuant to a will, applicable intestacy rules, etc.
2. The request will be forwarded to the former employee’s unit.
3. 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.
4. The initial request and subsequent approval must be submitted to the Chief Information Security Officer (ciso@uoregon.edu).
5. Live access to any electronic communications system or account shall not be provided.
6. All personal electronic communications records can be made available to the requestor.
7. University work-related electronic communications 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 significant 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. For purposes of this Procedure, an electronic file that has not been transmitted is not an electronic communication.

**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 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.

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

**Possession of Electronic Communications Record**: An individual is in possession of an electronic communications 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 communications record that resides on an electronic communications 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 communications not specifically created by or addressed to them.

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

**Substantiated Reason**: Reliable evidence indicating that violation of law or of University policies probably has occurred, as distinguished from rumor, gossip, or other unreliable evidence.

**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.