Reason for Policy

The University of Oregon ("university" or "UO") values our community's right to privacy, safeguards personal information, and ensures the appropriate institutional use of personal information provided to or maintained by the university. This policy defines some common terms and outlines the reasonable expectations of privacy throughout the collection, storage, use, and disclosure of personal information provided to or maintained by the university.

Entities Affected by this Policy

This policy applies to the university as an enterprise, including but not limited to all university offices, units, and departments that collect, store, use, disclose or manage data related to UO employees, students, alumni, retirees, volunteers, visitors, contractors, vendors, customers, certain third parties, and research subjects. This policy provides the minimum baseline guidance regarding the reasonable expectation of privacy in the absence of more detailed legal, policy, or contractual requirements.

Web Site Address for this Policy

[Provided by Office of the University Secretary after policy is posted online]

Responsible Office

For questions about this policy, please contact the Office of the Chief Information Security Officer, (541) 346-1701, or ciso@uoregon.edu.

Enactment & Revision History

Day-Month-Year – [text]
Day-Month-Year – [text]

Definitions

In this policy, unless otherwise defined by applicable law, the following definitions apply:

"*Disclosure*" means the release, transfer, provision of, access to, or divulging in any other manner, of information outside the UO office, unit, or department storing, or maintaining the personal information. "Disclose" has the corresponding meaning.

"*Personal information*" means any recorded information or data that is about an individual person and from which that person can be identified. It does not include information where an individual person's identity has been removed (e.g. anonymous or redacted information).

"*Personal information processing*" means anything that any individual acting on behalf of the university does with the personal information – including but not limited to collection, use, storage, disclosure, conversion, migration, deletion, or retention.

"*Information Technology (IT) System*" means an information system, a communications system, or, more specifically, a computer system — including but not limited to all hardware, software, and peripheral equipment — operated by a limited group of IT users.

"(IT) System Maintenance" means a set of actions to ensure that an IT system remains secure and operational. It typically involves three main maintenance types: preventive, corrective, and proactive. Preventive maintenance focuses on routine tasks to prevent system issues (e.g., software updates and security patches). Corrective maintenance addresses problems as they arise, such as repairing or replacing parts. Proactive maintenance seeks to improve system performance and longevity by upgrading software or hardware when necessary, ensuring systems continue to run efficiently.

"*University Privacy Officer Representative*" means the function of a university employee in the Information Security Office who is responsible for responding to inquiries about data privacy. The University Privacy Officer Representative can be reached at privacyofficer@uoregon.edu.

Policy

The University of Oregon is committed to protecting personal information and the reasonable expectation of privacy to the extent possible, subject to state and federal law. The university limits the collection, use, sharing, and storage of personal information except where reasonably necessary to serve the institution's academic, research, or administrative functions, including but not limited non-UO external third parties who contract with the university to help administer its operations~~,~~ or other legally permitted purposes. Such collection, use, sharing, and storage must comply with applicable laws, rules and regulations, as well as the policies, standards, and procedures of the university. Other than as stated above, or as required by legal or regulatory requirements that guarantee public access to certain types of information (e.g., laws, regulations, valid subpoenas, applicable legal instruments), personal information is not actively disclosed to non-UO external third parties.

Reasonable Expectations of Privacy of Personal Information

While information collected, used, disclosed, and stored by the university is UO's public property and may reasonably be subject to the Oregon Public Records Law outlined at ORS Chapter 192 without a reasonable expectation of privacy, the university recognizes a reasonable expectation of privacy may exist for some personal information subject to applicable laws and university policies and procedures. While the university strives to protect personal information and uses reasonable technical, organizational, and administrative efforts to do so, it cannot guarantee absolute privacy of all such information. In addition to the above-mentioned institutional purposes, individuals can expect personal information to be used by the institution under the following circumstances:

- System maintenance or administrative, academic, and research operations, including but not limited to security measures;
- valid consent from the individual to share their information;
- provision of university services internally or by non-UO third parties;

- disclosure to protect the health, safety, or property of any individual or in the event of an emergency facing the university;
- investigation of suspected violations of legal requirements or institutional policy;
- fulfillment of legal obligations under Oregon Public Records Law or other applicable laws, regulations, subpoenas, orders, or institutional policies, rules, or guidelines; and
- as permitted by applicable law or policy.

Privacy Notice

The university will maintain and publish a privacy notice to describe, at a minimum, the type of information the university collects, how the information is used, and to whom the information is or may be disclosed. This applies to the collection of general information and personal information. The notice will be posted in conspicuous locations including but not limited to the university's websites.

Responsibilities

a. Data and information privacy are the shared responsibility of all members of the university community. All members of the university community are expected to follow and support the university's privacy policy and associated procedures.
b. The provost and vice presidents are responsible to ensure implementation and enforcement of this policy in all IT systems and services within their respective portfolios.
c. All administrators, deans, department heads, directors, supervisors and/or principal investigators are directly accountable for maintaining the privacy of personal information that is collected in areas for which they are responsible. This includes but is not limited to the establishment and management of data privacy procedures as well as ongoing support by each unit for data privacy, including but not limited to appropriate training on data protection strategies and tools.
d. The Information Security Office is responsible for providing training, technical expertise and assistance to campus partners regarding compliance with laws, regulations, and policies associated with the protection of personal and other protected data.
e. All employees are responsible for reporting all data disclosures and incidents, unintended or otherwise, involving unauthorized access to personal information. Such a report shall be made to an immediate supervisor who shall report the situation to the appropriate person or office for action. Additionally, it can be directly reported to the University Privacy Officer Representative.

Related Resources

University of Oregon Privacy Notice
Information Asset Classification & Management Policy
Data Security Incident Response Policy