Policy Title: Data Access

Responsible University Office:

University Office: Information Services
Office Website URL: http://it.uoregon.edu/is/home
Policy Owner: Melissa Woo, Chief Information Officer and Provost for Information Services
Email: mwoo@uoregon.edu
Phone: 541-346-1702
Date: November 26, 2012

Policy Concept Form: The policy concept form was approved by the Senior Vice President and Provost on the following date:

As part of the Integrated Data & Reporting project, the University of Oregon Interim Provost appointed a Data Policy subcommittee on December 15, 2011, to establish data compliance policies for all university data. This policy is part of that charge.

NOTE: Policy development may not proceed until the policy concept has been approved.

Preamble:
The University of Oregon (UO) adopts this policy to protect the University’s information assets and business processes.

Reason for Policy:
Authorized personnel may have a business need to access certain UO databases or other information assets in order to complete necessary work-related tasks. The UO has a responsibility to protect information entrusted to it, ensure the effective operation of business critical processes, and comply with the security policies established by the State Board of Higher Education, and comply with other state and federal laws. The purpose of this policy is to set forth the terms and conditions under which authorized personnel may have access to information assets.

Definitions:

"Business Need" is established if a UO employee has a demonstrably legitimate need to access specific information assets such as paper files, computer networks, email accounts or other data sources in order to fulfill their official, professional responsibilities.

"Data" is information stored electronically or in print.
“Due Care” is the conduct that a reasonable person will exercise in a particular situation in looking out for the safety of others. Due care includes the conduct that a reasonable person will exercise in a particular situation to protect UO’s information assets.

“Sensitive Information Assets” are those information assets that the UO is obligated by law or contract to protect or that represent confidential data that, if released, would represent some actual legal or business liability to the UO.

"Information Assets" includes data and other information and systems that are owned or controlled by UO, information that UO is obligated to keep secure or confidential by applicable law or contract, and information exempt from disclosure under public records laws. UO information assets may exist in written, spoken, electronic, printed, magnetic, optical, and other mediums.

“Authorized Personnel” are persons, including employees, students, vendors, visitors, affiliates, and courtesy faculty, who have been authorized by UO to interact with information assets.

“Data Owner” is the Provost or the Provost’s designee.

“Remote Access” is the authorized and secure access of UO resources and functionalities from other than a UO IP address.

“VPN” or “Virtual Private Network” is a system for encrypting network traffic between a user’s local computer system and another remote computer system.

**Policy Statement:**

**General Access to Information Assets**

Only authorized personnel may have access to the information assets. Such access may be granted only to the extent and for such time that a business need exists. Access shall be limited, using technical or procedural controls, to the least permission necessary for the performance of duties. The data owner is responsible for determining who may be granted access to data and information assets for which the data owner is responsible. A record of the request for access and grant of authority to access data or information assets shall be maintained by the data owner. It is the responsibility of all authorized personnel to protect data and information assets from unauthorized change, destruction or disclosure.

Procedures should be implemented by the Vice Provost for Information Services:

- to authorize access, both logical and physical, only to Authorize Personnel who have a business need to access specific data or other information assets;
- to modify access as appropriate, including when duties change;
- to revoke access upon termination of UO status or when duties no longer require a legitimate business reason for access;
- to ensure that all authorized personnel sign and date the UO Code of Responsibility for Security and Confidentiality of Records and Files indicating their agreement to comply with its terms and conditions. However, failure to sign or date the UO Code of Responsibility does not render anyone exempt from such compliance obligation; and
- to provide appropriate confidentiality and security training to authorized personnel.

Department heads and other Unit administrators must notify relevant data owners of activities or changes that
Authorization and access must be removed for authorized personnel whose employment has been terminated, who have received notice of termination or nonrenewal, or who have announced their decision to terminate employment, unless an exception has been authorized by the relevant appointing authority.

Remote Access to Information Assets

Remote access to information assets may only be provided through a secured system approved by the Chief Information Officer of the University.

Remote access is provided only under a business need basis. Remote access is subject to the approval of the data owner. An employee who is subject to state or federal overtime compensation requirements may be granted remote access only if he or she agrees in writing not to work any hours that will result in overtime compensation being due, unless doing so is authorized in advance by the employee’s supervisor.

Exclusions and Special Situations:

Procedures:
Information System (IS) recommendations for access to financial, student and employee data can be found at http://it.uoregon.edu/node/2944

Additional information on procedures and information access will be maintained at the following:
- Banner http://it.uoregon.edu/services/banner
- Data Warehouse http://it.uoregon.edu/services/data-warehouse
- Integrated Data and Reporting (IDR) http://idr.uoregon.edu
- Banner access procedures http://bg.uoregon.edu/content/banner-access
- Document management system http://it.uoregon.edu/services/document-imaging

The most common type of remote access will be via a VPN that is authorized by and supplied by UO. Information about UO-VPN is available at http://it.uoregon.edu/vpn. Other information about required security protocols for remote access will be maintained and regularly updated at http://it.uoregon.edu/node/2944.

Forms/Instructions/Regulations:
OAR 580-055-0000 - 0080
OUS Fiscal Policy 56.350 Information Security

Who is Governed by this Policy:
(Please mark all that apply by double clicking on box)
- Faculty
- Officers of Administration
- Students
- Staff
- Other: Any other person allowed access UO information assets

Who Should Know this Policy:
All University personnel involved with using, requesting, approving, or accessing UO information assets.
Cross Reference to Related Policies:

Frequently Asked Questions:

Related Documents:

Frequently Asked Questions:

Revision/Development History:

Organizational Category:
(Please mark only one by double clicking on box)

- Administration and Governance
- Academic and Curricular
- Human Resources
- Facilities
- Students
- Finance and Business Affairs
- University Relations
- Health and Safety
- Research
- Information Technology
- General
POLICY CONSULTATION AND REVIEW

Consultation and review by the following individuals or groups:

Chief Information Officer & Vice Provost for Information Services: Date: 7/Dec/2012

Approved by Randy Geller by email Date: 10/26/2012
General Counsel

Senior Vice President and Provost Date: 12/19/12

University of Oregon Senate President Date: 1/24/2012

Click here to add Name or Group

APPROVED BY:

President or Designee Signature Date: 2/19/13

POLICY EFFECTIVE DATE: 2/19/13

ASSIGNED POLICY NUMBER: 10.00.01 kW
# Signature Routing & Request Form

**SUBJECT:** Data Access Policy

<table>
<thead>
<tr>
<th>Select for review</th>
<th>Administrator</th>
<th>Signature</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>VP for Finance &amp; Administration</td>
<td>[Signature]</td>
<td>1/28/13</td>
<td>Sec ond editing issue (above) - I think this is a typo.</td>
</tr>
<tr>
<td>☒</td>
<td>Office of the General Counsel</td>
<td>[Signature]</td>
<td>1/27/13</td>
<td>☒ Legal review not required</td>
</tr>
<tr>
<td></td>
<td>Athletic Director</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VP for Development</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VP for Enrollment Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VP for Institutional Diversity &amp; Inclusion</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VP for Research, Innovation &amp; Grad Studies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VP for Student Affairs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VP for University Relations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td>Others (specify)</td>
<td>[Signature]</td>
<td>2/18/13</td>
<td>Typo corrected. &quot;with&quot; left out of reason section - &quot;comply with the security policies&quot;. Rob Key notified of correction. Kathy wagon</td>
</tr>
<tr>
<td>☐</td>
<td>Others (specify)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>After all other signatures, please route to the Provost then President for final review/approval</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td>Senior VP &amp; Provost</td>
<td>Jim Bean has approved and signed the policy. KW</td>
<td></td>
<td></td>
</tr>
<tr>
<td>☐</td>
<td>President</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Instructions: Originating office should select any other administrators they think should be included in the review/approval loop. In all cases review and signature are required from the VPFA, General Counsel, Provost, and ultimately the President. Feel free to re-order administrators based on the originating office and preferred order of review, expand comments field, etc. Please contact Staci Knabe with questions.
Rob, just letting you know that I made a minor correction to the policy. A word was left out of the “Reason for Policy” section. You can see the correction in red in the section below:

*Reason for Policy:*

*Authorized personnel may have a business need to access certain UO databases or other information assets in order to complete necessary work-related tasks. The UO has a responsibility to protect information entrusted to it, ensure the effective operation of business critical processes, and comply with the security policies established by the State Board of Higher Education, and comply with other state and federal laws. The purpose of this policy is to set forth the terms and conditions under which authorized personnel may have access to information assets.*

Thanks.

Kathy Warden  
Program Manager  
Office of the Senior Vice President and Provost  
University of Oregon  
(541)346-3531