



***State Board of Higher Education***

P.O. Box 3175  
Eugene, OR 97403-0175  
FAX: (541)-346-5790  
PHONE: (541)-346-5749

March 25, 2009

TO: MEMBERS OF THE STATE BOARD OF HIGHER EDUCATION

Meetings of the State Board of Higher Education will be held on April 2-3, 2009. On Thursday, the OUS Research Council will be meeting from 10 a.m. until noon in conference room 511 of PSU's Urban Center, 506 SW Mill St, Portland, Oregon.

Also scheduled for Thursday is the Board's visitation at Western Oregon University, beginning at 4 p.m. in the Smith Music Hall Auditorium, room 121.

The Board will convene a regular meeting at 8 a.m. on Friday, April 3<sup>rd</sup>. Agenda items include: the approval of OIT's proposal to offer an instructional program leading to a master of science degree in civil engineering. Three items have been presented for action: the System's Identify Theft Prevention policy, changes to IMD 6.140(2) relating to endowment fund investments, and the proposed Board committee charters. The Board will hear several reports, including a presentation from OSU's extension service and updates from the Board's Student Participation and Completion Committee and the Tuition Policy Work Group. The agenda also includes discussions on undergraduate program demand and minimum class size policies and the common admissions process for OUS institutions.

Additionally, the Chancellor, the president of the Interinstitutional Faculty Senate, and the chair of the Oregon Student Association will provide informational reports to the Board. This meeting will be held in accordance with the time, location, and schedule listed below:

Friday, April 3, 2009, Werner University Center  
8 a.m. – 2:30 p.m. Full Board meeting, Pacific Room

Telephone messages for Board members and institution officials attending the meetings may be called to (541) 554-6450. If special accommodations are required, please contact the Board's Office at (541) 346-5749 at least 72 hours in advance. All docket materials are available on the OUS website at [http://www.ous.edu/sb\\_meet.htm](http://www.ous.edu/sb_meet.htm).

Cordially,

A handwritten signature in black ink, appearing to read 'Ryan J. Hagemann', written over a white rectangular box.

Ryan J. Hagemann  
Secretary of the Board

## Directions to Western Oregon University

Address ..... 345 N. Monmouth Ave., Monmouth, OR 97361  
Switchboard ..... 503-838-8000  
Office of Disability Services..... 503-838-8250  
Central Fax ..... 503-838-8474

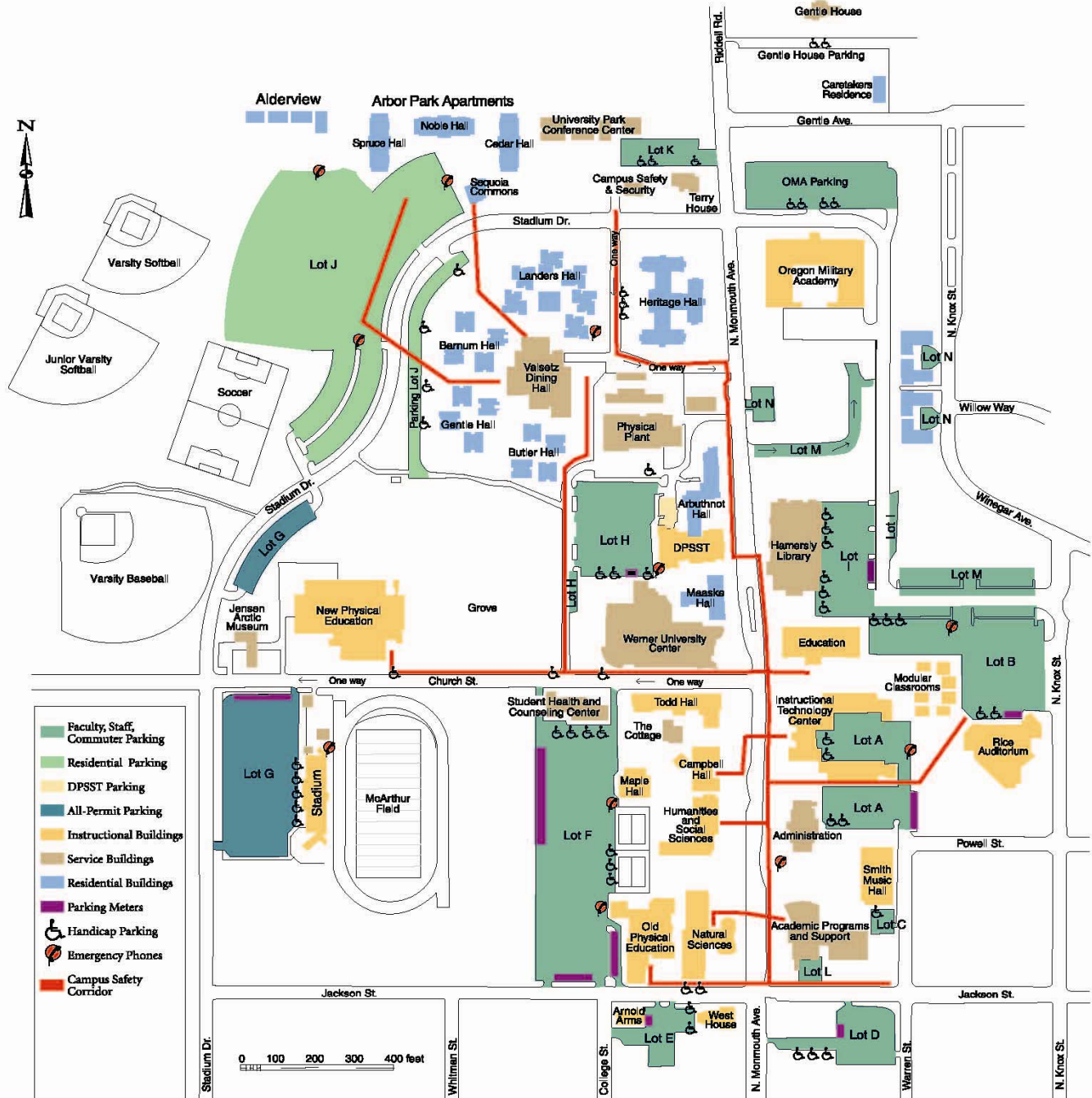
**Interstate 5 Northbound:** Take Exit 249 (Commercial Street). Follow Commercial into Salem, and as you near downtown, Commercial will curve to the right and become Liberty Street. Stay on Liberty until you reach Marion Street. Turn left, cross the Marion Street Bridge on to Highway 22, and follow the signs marked “Dallas/Ocean Beaches.” Stay on Highway 22 until you reach Highway 99W. Take exit 16 on the right side of the overpass that puts you on Highway 99W. Go south about six miles to Monmouth. Take a right onto Main Street at the stop light. Follow Main Street west to Monmouth Avenue and turn right.

**Alternate Northbound Route:** Take Exit 228 and follow route 34 towards Corvallis. After crossing the Willamette River into Corvallis, turn right at the second light onto scenic highway 99W. Continue north about 20 miles until you reach Monmouth; turn left at the first stop light, onto Main Street. Follow Main Street west to Monmouth Avenue and turn right.

**Interstate 5 Southbound:** Take Exit 260A (Salem Parkway). Follow the Parkway into Salem. The Parkway will curve to the left and become Commercial Street. Stay on Commercial until you reach Marion Street. Turn right, cross the Marion Street Bridge on to Highway 22, and follow the signs marked “Dallas/Ocean Beaches.” Stay on Highway 22 until you reach Highway 99W. Take exit 16 on the right side on the overpass that puts you on Highway 99W. Go south about six miles to Monmouth. Take a right onto Main Street at the stop light. Follow Main Street west to Monmouth Avenue and turn right.

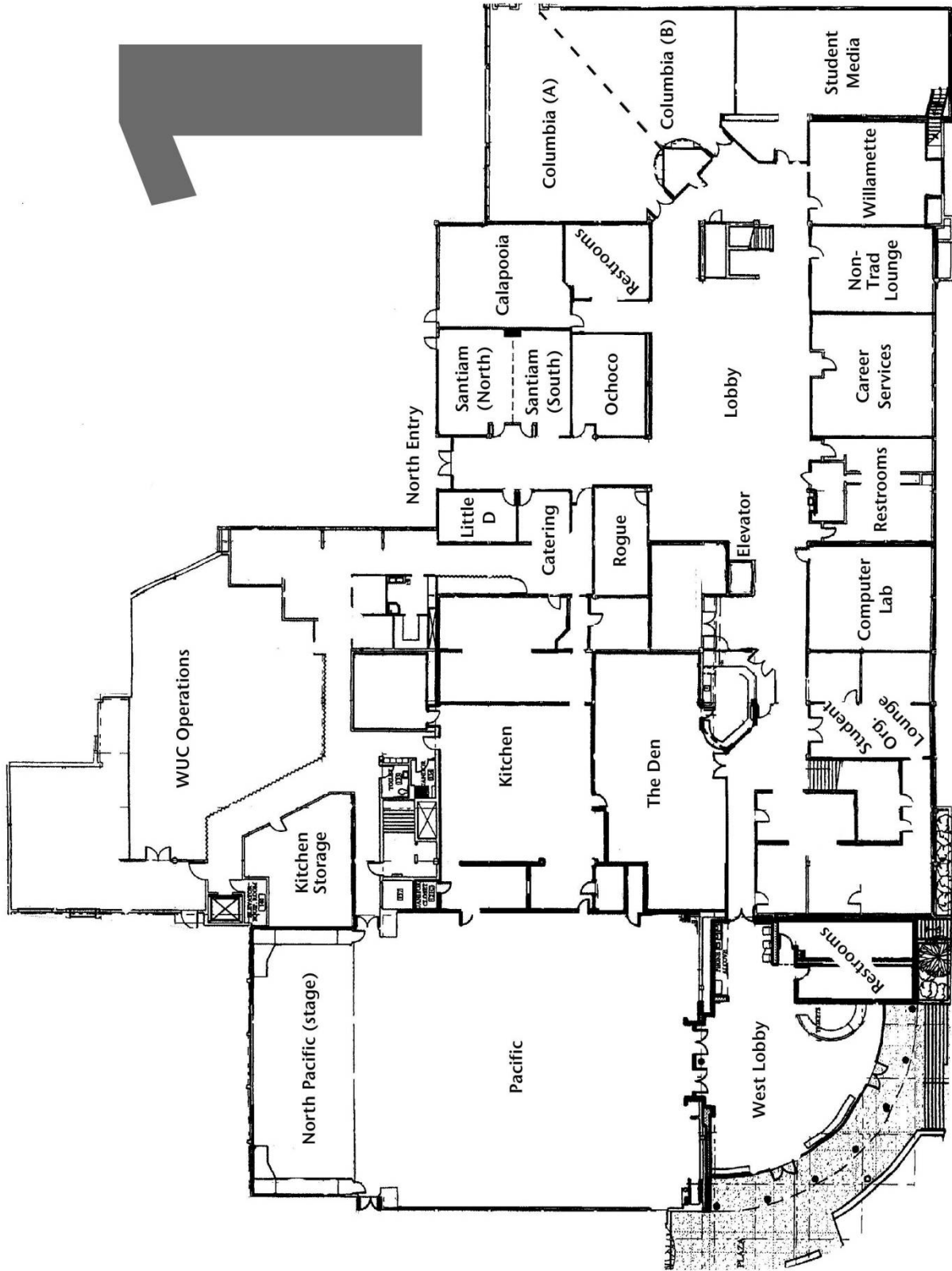


Please park in the designated spaces in Parking Lot H, behind the university center.





Werner University Center, First floor floorplan.





OREGON STATE BOARD OF HIGHER EDUCATION  
WERNER UNIVERSITY CENTER  
WESTERN OREGON UNIVERSITY  
MONMOUTH, OREGON



REGULAR MEETING OF THE STATE BOARD OF HIGHER EDUCATION  
PACIFIC ROOM, WERNER UNIVERSITY CENTER  
MONMOUTH, OREGON  
APRIL 3, 8 A.M. – 2:30 P.M.

AGENDA

1. CALL TO ORDER/ROLL CALL/WELCOME

2. REPORTS

- a. Chancellor’s Report
- b. Interinstitutional Faculty Senate (IFS) President (Gilkey)
- c. Oregon Student Association (OSA) Chair

3. CONSENT ITEMS

- a. [OIT, M.S. in Civil Engineering](#) ..... 1  
Oregon Institute of Technology seeks Board approval to offer an instructional program leading to a M.S. in Civil Engineering.

4. ACTION ITEMS

- a. [OUS, Identity Theft Prevention Program \(Green\)](#) ..... 5  
For compliance with the *Red Flag Rule* under sections 114 and 315 of the Fair and Accurate Credit Transactions Act, the proposed Identity Theft Prevention Program will identify potential red flags that signal identity theft, detect the occurrence of identified red flags, and will appropriately respond to these detected red flags.
- b. [OUS, Update to IMD 6.140\(2\) Relating to Endowment Fund Investments \(Green\)](#) ..... 15  
This is a housekeeping item that does not change endowment fund investment management.
- c. OUS, Approval of Proposed Board Committees (Kelly/Hagemann)

**5. REPORT ITEMS**

- a. OSU Extension Services Report (Vice Provost Scott Reed)
- b. Tuition Policy Work Group Update (Fox/Kenton)
- c. Student Participation and Completion Committee Update (Miller-Jones)

**6. DISCUSSION ITEMS**

- a. OUS, Policies on Undergraduate Program Demand and Minimum Class Size (Weeks)
- b. OUS, Common Admissions Process for OUS Institutions (Holliday)  
Development of a common admissions application question and applicant release of information for all seven universities to facilitate acceptance and aid packaging at other OUS institutions prior to notification of denial of admission.

**7. COMMITTEE REPORTS**

- a. Standing Committee Reports
- b. Other Board Committees

**8. PUBLIC INPUT**

**9. BOARD COMMENTS**

**10. DELEGATION OF AUTHORITY TO BOARD'S EXECUTIVE COMMITTEE**

“Pursuant to Article II, Section 5 of the Bylaws of the Board of Higher Education, the Board delegates to the Executive Committee authority to take final action as here designated or deemed by the committee to be necessary, subsequent to the adjournment of this meeting and prior to the Board's next meeting. The Executive Committee shall act for the Board in minor matters and in any matter where a timely response is required prior to the next Board meeting.”

**11. ADJOURNMENT**

*Note: All docket materials are available on the OUS website at: [http://www.ous.edu/state\\_board/meeting/index.php](http://www.ous.edu/state_board/meeting/index.php). Please contact the Board's office at (541) 346-5749 if you have any questions regarding these materials. This agenda may be amended at any time prior to 24 hours before the Board meeting. Estimated starting times for the agenda items are indicated; however, discussions may commence, or action may be taken, before or after the suggested times. Any item on the agenda may be considered at any time out of order at the discretion of the President of the Board. During the meeting, the Board may convene in Executive Session to receive legal advice regarding any item on the agenda or for any reasons permitted under Oregon law.*



Oregon  
University  
System

# **Oregon State Board of Higher Education**

April 3, 2009  
Western Oregon University  
Monmouth, Oregon

Board Materials

**REGULAR MEETING #826 OF THE OREGON STATE BOARD OF HIGHER EDUCATION  
PACIFIC ROOM, WERNER UNIVERSITY CENTER, WESTERN OREGON UNIVERSITY  
MONMOUTH, OREGON  
APRIL 3, 2009**

**TABLE OF CONTENTS**

	<u>Page</u>
OIT, M.S. in Civil Engineering .....	1
OUS, Identity Theft Prevention Program .....	5
OUS, Update to IMD 6.140(2) Relating to Endowment Fund Investments.....	15

(This page intentionally left blank.)

## OIT, M.S. in Civil Engineering

1. *Describe the purpose and relationship of the proposed program to the institution's mission and strategic plan.*

Preparing students to become licensed professional engineers has long been the primary goal of the Civil Engineering Department at Oregon Institute of Technology (OIT). As the licensure requirements have changed over the years, so has the program: most notably with the transition from offering degrees in civil engineering technology to degrees in civil engineering because, throughout the United States, many of the state boards were no longer granting licenses to practitioners with technology degrees. The industry is undergoing yet another major philosophical shift in that the American Society of Civil Engineering (ASCE), the National Council of Examiners for Engineering and Surveying (NCEES), and Accreditation Board for Engineering and Technology (ABET) are each pursuing various policies requiring graduate degrees (or equivalent coursework) in order to be eligible for professional licensure. As such, the addition of a graduate civil engineering program at OIT is a logical way to continue the current mission.

The current institutional mission statement, approved by the Oregon Board of Higher Education, is comprised of six central objectives. These are listed below with a short description of how the proposed program supports each one.

- Provide degree programs that enable graduates to obtain the knowledge and skills necessary for immediate employment. A majority of the employers of graduates from the Bachelor of Science in Civil Engineering (BSCE) program at OIT are seeking to hire individuals who will be eligible for professional licensure. As discussed previously, candidates in the near future will need to obtain a master's degree (or equivalent) to be eligible and so offering a Master of Science in Civil Engineering (MSCE) is going to be integral to a graduate's employability.
- Enable students to be effective communicators, responsible citizens, and lifelong learners by assisting them in the development of critical thinking and problem solving skills, and ethical and cultural awareness. Providing students with access to advanced coursework and projects will strengthen their communication, critical thinking, and problem solving skills as well as give them more exposure to an increasingly broad industry.
- Offer continuing and distance education and advanced professional studies to meet the emerging needs of today's citizens. Offering advanced courses in civil engineering will provide continuing education to today's citizens.
- Provide informational and technical expertise to regional, state, national, and global publics in applied research. It is expected that a majority of the students pursuing the MSCE degree will conduct a significant applied research project, the results of which will be disseminated to the general public via papers and presentations at both the regional and national level.
- Develop and maintain partnerships with public and private institutions, business and industry, and government agencies to ensure quality programs

- that meet the needs of students and the organizations that employ them. Current partners strongly support the offering of a MSCE at OIT.
- Provide statewide access to address the needs of the Oregon workforce. The proposed MSCE would only be offered at the Klamath Falls OIT campus. Other MSCE programs are available in northern Oregon.

2. *What evidence of need does the institution have for the program?*

As the Oregon economy improves, more construction takes place. As more buildings, bridges, roads, and communities are being built, the need for civil engineers to design these systems grows as well. Unlike other fields of engineering, civil engineering is less often outsourced. The result of these two factors is the fact that the need for civil engineers in Oregon has increased dramatically in recent years. According to *The Oregonian*: “public and private employers throughout the region are struggling to attract qualified civil engineers from a small pool of candidates.” Nationally, *USA Today* states that due to “general population growth and an expanding economy, more civil engineers will be needed to design and construct higher capacity transportation, water supply, pollution control systems, and large buildings and building complexes.” Furthermore, a national career development and job search association lists civil engineering as being in the top 10 most in demand degrees for 2007.

3. *Are there similar programs in the state? If so, how does the proposed program supplement, complement, or collaborate with those programs?*

Both Oregon State University and Portland State University have a M.S. in Civil Engineering. It is intended that the OIT’s MSCE program would be complementary to and not in competition with the MSCE programs offered at Oregon State University and Portland State University. The OUS Provost’s Council has approved this degree.

There is no projected student enrollment or faculty workload impact on other OUS institutions.

4. *What new resources will be needed initially and on a recurring basis to implement the program? How will the institution provide these resources? What efficiencies or revenue enhancements are achieved with this program, including consolidation or elimination of programs over time, if any?*

Initially, enrollment in the program will be low and, as such, it is estimated that no additional faculty members will be needed. As the program grows, and especially if Oregon and/or surrounding states require an M.S. or equivalent for licensure, an additional faculty member will be required. Specifically, it is estimated that when PS 465 is implemented fully, 95 percent of the BSCE students at OIT will remain for an MSCE as well. When this happens, it will be necessary to add another assistant, associate, or full professor with as broad a background within the area of civil engineering as possible to further support the objective to prepare students for

professional practice. Because the NCEES model law calls for a 2015 implementation, which, when subtracting four years of professional practice from that number, would affect students graduating in 2011, it is estimated that an additional faculty member would be required in the fall of 2011.

The OIT Library's holdings in the broad subject category of civil engineering include print and electronic resources. In recent years, the Library has purchased more journals and books electronically in response to cost savings for electronic titles over printed editions and cost savings through consortial buying opportunities. To bring library materials to an appropriate level for this program will require initial funds of \$5,000. The majority of this additional financial support will be through a reallocation of a portion of the Library budget that is dedicated to the Civil Engineering Department. Other funding will come from external research grants.

Facilities, Equipment, and Technology: In the program's infancy, because initial enrollment will be low, few additional resources will be required. As the program grows, however, especially with the full implementation of PS 465, it is envisioned that some additional facilities and equipment will be needed. Specifically, some graduate student offices and updated lab equipment would be beneficial.

The Department has had great success obtaining lab equipment from a number of different sources. Grants from private groups, such as the Associated General Contractors of America, which provides an annual equipment grant, are expected to continue to provide updated and additional equipment.

All appropriate University committees and the OUS Provosts' Council have positively reviewed the proposed program.

*Recommendation to the Board:*

The OUS Provosts' Council recommends that the Board authorize Oregon Institute of Technology to establish an instructional program leading to a M.S. in Civil Engineering, effective Fall 2009.

**(Board action required.)**

(This page intentionally left blank.)

## **OUS, Identity Theft Prevention Program**

### Background

In late 2007, the Federal Trade Commission (FTC) and Federal banking agencies issued a regulation known as the *Red Flag Rule* under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. (A “Red Flag” is defined as a pattern, practice, or specific activity that indicates the possible existence of identity theft.) The regulation is intended to reduce the risk of identity theft that results in the theft of goods and/or services that are provided by creditors to their customers on account.

The regulation applies to any organization that allows its customers to obtain goods and/or services and defer payment for those goods or services. The Red Flag rule requires any such organization to establish, document, and maintain an Identity Theft Prevention Program (Program) that identifies potential red flags that signal identity theft, detects the occurrence of identified red flags, and appropriately responds to detected red flags.

The regulation requires that the Program be approved by the organization’s governing board. Oversight of the program is to be assigned to a senior management level staff member, with program reviews conducted annually. Red Flag rules go into effect on May 1, 2009.

### Program Development

The Chancellor’s Office developed a draft Program based on examples from other universities and the National Association of College and University Business Officers (NACUBO). The Chancellor’s Office then engaged a team consisting of the director of business affairs at each campus, the OUS General Counsel, the general counsels from Oregon State University and the University of Oregon, and a representative from Information Technology to further refine the Program. The Program that is presented as [Attachment A](#) was then reviewed and approved by the vice presidents for finance and administration at each campus.

### Risk Assessment

The campus representatives to the Program development process reported no known instances of identity theft relating to deferred payment programs that resulted in the theft of goods and/or services from their campuses. While the team believes the likelihood of such identity theft is remote, the team also believes that the risk is growing with the advent of electronic account access coupled with automated financial aid refund processes. Campuses currently employ strong processes and procedures that significantly reduce the risk of this type of identity theft. Examples include requiring photo identification for registration and financial aid disbursement and securing electronic systems via password and other authentication processes. The OUS administration concludes that the risk of identity theft relating to deferred payment programs that result in the theft of goods and services to be low.

*Administration of the Program*

The Program establishes an Identity Theft Committee (Committee), appointed by the vice chancellor for finance and administration, to implement and administer the provisions of the Program. The Committee will be made up of a Chancellor's Office representative and a Program administrator for each OUS campus. The Program administrators will be responsible to implement and administer the Program at their campus. The Committee will review the Program annually (or more frequently if events warrant) to review its effectiveness and to determine if changes in the Program are needed. The Program must be implemented by May 1, 2009.

*Staff Recommendation to the Board:*

Staff recommends that the Board adopt the attached Identity Theft Prevention Program.

**(Board action required.)**

**Attachment A**

Oregon University System  
Identity Theft Prevention Program  
Effective May 1, 2009

## I. PROGRAM ADOPTION

The Oregon University System (“System”) developed this Identity Theft Prevention Program (“Program”) pursuant to the Federal Trade Commission’s (“FTC”) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with oversight and approval of the Oregon University System Board. After consideration of the size and complexity of the System’s operations and account systems, and the nature and scope of the System’s activities, the Board determined that this Program was appropriate for the System, and therefore approved this Program on April 3, 2009.

## II. PURPOSE

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a new covered account or the use of an existing covered account and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts the System offers or maintains and incorporate those red flags into the program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

## III. DEFINITIONS AND PROGRAM

### A. Red Flags Rule Definitions Used in this Program

“Identity Theft” is a “fraud committed or attempted using the identifying information of another person without authority.”

A “Red Flag” is a “pattern, practice, or specific activity that indicates the possible existence of Identity Theft.”

A “Covered Account” is an account that the System maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.

The “Program Administrator” is the individual designated with primary responsibility for oversight of the program. See Section VI below.

“Identifying information” is “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including: name, address, telephone number, social security number, date of birth, government issued

driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, or routing code.

### **B. Fulfilling Requirements of the Red Flags Rule**

Under the Red Flags Rule, the System is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. The program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to students or to the safety and soundness of the student from identity theft.

The Red Flags Rule allows the System to base its program on the relative risks of identity theft in connection with its covered accounts. Based on the experience of its member institutions, the System considers the risk of identity theft in connection with its covered accounts to be low. Accordingly, this Program has been developed based on that assessment of risk.

## **IV. COVERED ACCOUNTS**

The System has identified 11 types of accounts, one of which is covered accounts administered by the System and multiple types of account that are administered by service providers.

System-covered accounts:

1. Refund of credit balances involving student loans
2. Deferment of tuition payments
3. Emergency loans
4. Bookstore charges
5. Student Health Center Charges
6. Federal Family Education Loan Program (FFELP) – (Stafford & PLUS)
7. Federal Perkins Loan Program
8. Jesse M. Bell Memorial Loan Fund
9. Revolving Charge Account Plan
10. William D. Ford Federal Direct Loan Program

Service provider-covered accounts:

1. "Higher One" Refund Disbursement Program – with Debit Card (refer to Section VIII(C) for oversight of service provider arrangements)

## V. IDENTIFICATION OF RELEVANT RED FLAGS

The Program considers the following risk factors in identifying relevant red flags for covered accounts:

1. The types of covered accounts as noted above;
2. The methods provided to open covered accounts—acceptance to System campuses and enrollment in classes may require some or all of the following information, subject to campus admission policies and student enrollment status:
  - a. Common application with personally identifying information;
  - b. High school transcript;
  - c. Official ACT or SAT scores;
  - d. Two letters of recommendation;
  - e. Entrance Medical Record;
  - f. Medical history;
  - g. Immunization history; and
  - h. Insurance card.
3. The methods provided to access covered accounts:
  - a. Disbursement obtained in person require picture identification; and
  - b. Disbursements obtained by mail can only be mailed to an address on file.
4. The System's previous history of identity theft.

The System identifies the following Red Flags in each of the listed categories:

### A. Notifications and Warnings from Credit Reporting Agencies

#### Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on an applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant;
4. Receipt of a notice of address discrepancy in response to a credit report request; and
5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

### B. Suspicious Documents

#### Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing student information; and
4. Application for service that appears to have been altered or forged.

### **C. Suspicious Personal Identifying Information**

#### **Red Flags**

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
2. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
3. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
4. Social security number (SSN) presented that is the same as one given by another student; and
5. A person fails to provide complete personal identifying information on an application when reminded to do so.

### **D. Suspicious Covered Account Activity or Unusual Use of Account**

#### **Red Flags**

1. Change of address for an account followed by a request to change the student's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail sent to the student is repeatedly returned as undeliverable;
5. Notice to the System that a student is not receiving mail sent by the System;
6. Notice to the System that an account has unauthorized activity;
7. Breach in the System's computer system security; and
8. Unauthorized access to or use of student account information.

### **E. Alerts from Others**

#### **Red Flag**

1. Notice to the System from a student, identity theft victim, law enforcement, service provider, or other source that the System has opened or is maintaining a fraudulent account for a person engaged in identity theft.

## **VI. DETECTING RED FLAGS**

### **A. Student Enrollment**

In order to detect any of the Red Flags identified above associated with the enrollment of a student, System personnel will take the following steps to obtain and verify the identity of the person opening the account:

#### **Detect**

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
2. Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification) or

follow identification verification processes administered by service providers for covered accounts.

## **B. Existing Accounts**

In order to detect any of the red flags identified above for an existing covered account, System personnel will take the following steps to monitor transactions on an account:

### **Detect**

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes; and
3. Confirm changes in banking information given for billing and payment purposes.

## **C. Consumer (“Credit”) Report Requests**

In order to detect any of the red flags identified above for an employment or volunteer position for which a credit report is sought, System personnel will take the following steps to assist in identifying address discrepancies:

1. Require verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the System has reasonably confirmed is accurate.

## **VII. PREVENTING AND MITIGATING IDENTITY THEFT**

In the event System personnel detect any identified red flags, such personnel shall take one or more of the following steps, depending on the degree of perceived risk posed by the red flag:

### **Prevent and Mitigate**

1. Continue to monitor a covered account for evidence of identity theft;
2. Contact the student or applicant (for which a credit report was run);
3. Change any passwords or other security devices that permit access to covered accounts;
4. Limit the use of SSN to what is absolutely necessary;
5. Notify any service provider with covered account;
6. Not open a new covered account;
7. Provide the student with a new student identification number;
8. Notify the Program Administrator for determination of the appropriate step(s) to take;

9. Notify law enforcement;
10. File or assist in filing a Suspicious Activities Report (“SAR”); or
11. Determine that no response is warranted under the particular circumstances.

### **Protect Student Identifying Information**

In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the System will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing student identity information when a decision has been made to no longer maintain such information;
3. Ensure that office computers with access to covered account information are password protected;
4. Use encryption and firewall technology;
5. Avoid use of social security numbers (See OUS Information Security Policy);
6. Ensure computer virus protection is up to date; and
7. Require and keep only the kinds of student information that are necessary for System purposes.

## **VIII. PROGRAM ADMINISTRATION**

### **A. Oversight**

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee (“Committee”) for the System. The Committee is appointed by the Vice Chancellor for Finance and Administration and will be made up of a Chancellor’s Office representative and a Program Administrator from each OUS campus. The Program Administrator at each campus will be responsible for ensuring appropriate training of System staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

### **B. Staff Training and Reports**

System staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. System staff shall be trained, as necessary, to effectively implement the Program. System employees are expected to notify the Program Administrator at their campus once they become aware of an incident of identity theft or of the System’s failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, System staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator on compliance with this Program. The report should

address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the Program.

### **C. Service Provider Arrangements**

In the event the System engages a service provider to perform an activity in connection with one or more Covered Accounts, the System will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the System's Program and report any Red Flags to the Program Administrator or the System employee with primary oversight of the service provider relationship.
3. Require, by contract, that service providers formally acknowledge and accept relevant and specifically identified provisions within the System's Program.

### **D. Non-disclosure of Specific Practices**

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation, and prevention practices may need to be limited to the Committee and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered "confidential" and should not be shared with other System employees or the public. The Program Administrator at each campus shall inform those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

### **E. Program Updates**

The Committee will periodically review and update this Program to reflect changes in risks to students and the soundness of the System from identity theft. In doing so, the Committee will consider the System's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the System's business practices and arrangements with other entities. After considering these factors, the Committee will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.

###

## **OUS, Update to IMD 6.140(2) Relating to Endowment Fund Investments**

### Background:

Prior to 2007, the OUS endowment funds were governed by Oregon's version of the Uniform Management of Institutional Funds Act (UMIFA). One of the provisions in UMIFA prohibited spending endowment funds below their original historic dollar value (HDV). In the 2007 legislative session, the Uniform Prudent Management of Institutional Funds Act (UPMIFA) was adopted to replace UMIFA. That law eliminated the prohibition on spending below the historic dollar value unless that provision was a part of the original trust document that created the endowment. The purpose of this change was to give institutions the ability to cope more easily with fluctuations in the value of the endowment. Under UPMIFA, institutions must still meet the general standard of prudence in their endowment investment decisions but they have more flexibility in establishing a spending policy that is responsive to short-term fluctuations in the market.

### Action Requested:

In order to provide the flexibility intended by UPMIFA, and bring the OUS policies in line with Oregon laws, the language in OUS Internal Management Directive (IMD) 6.140(2) that prohibits spending below HDV needs to be removed.

In addition, in reviewing IMD 6.140(2), it was noted that a reference to Section (1) of IMD 6.140 should be updated to reflect the current language therein. This is a housekeeping item that does not change endowment fund investment management.

### Staff Recommendation to the Board:

Staff recommends approval of the following changes to IMD 6.140(2); the added language is underlined and deleted language is in ~~strikethrough~~:

6.140(2) - Dividend and interest income in excess of the amount needed to fund the annual spending participant requirements specified in ~~6.140(1)~~ the investment objectives and policy guidelines approved by the Board are placed in an endowment fund reserve account and reinvested. Securities may be sold to provide cash equivalent to the income needs ; ~~however, the book value of endowments may not be invaded.~~

**(Board action is required.)**

(This page intentionally left blank.)