

**BOARD OF EDUCATION
UMPQUA COMMUNITY COLLEGE
DOUGLAS COUNTY, OREGON**

Information Item

Action Item

Subject: Consent Agenda

Date: April 8, 2020

Recommend approval of:

- 1. Minutes of College Board Meeting of March 11, 2020 pp 1-3
- 2. Minutes of Budget Committee Meeting of March 12, 2020 pp 4-7
- 3. Minutes of College Special Board Meeting of March 17, 2020 pp 8-9
- 4. Personnel Actions p 10
- 5. The following policies are coming to the Board for a second reading:

Old #	New #	Title	Page #
N/A	2432	Designation of Acting President	11
N/A	4010	Academic Calendar	12-13
344	4030	Academic Freedom	17-19
N/A	4106	Nursing Programs	23
600.08	5800	Prevention of Identity Theft in Student Financial Transactions	26-28

The associated administrative procedures are being shared as an information item:

Old #	New #	Title	Page #
N/A	4010	Academic Calendar	14-16
344	4030	Academic Freedom	20-22
N/A	4106	Nursing Programs	24-25
600.08	5800	Prevention of Identity Theft in Student Financial Transactions	29-54

- 6. Personnel Agreements pp 55-57

See separate Consent Agenda packet (pages 1-53) for the related documents.

Recommendation by:



Approved for Consideration:



**UMPQUA COMMUNITY COLLEGE BOARD MINUTES
March 11, 2020**

The Umpqua Community College Board of Education met on Wednesday, March 11, 2020, in Room 101 of the Bonnie J. Ford Health, Nursing, & Science Center at Umpqua Community College in Roseburg, Oregon. Board Chair Loosley called the meeting to order at 4:38 p.m. and the pledge of allegiance was given.

Directors present: Doris Lathrop, David Littlejohn, Guy Kennerly, Twila McDonald, Erica Mills, and Steve Loosley

Directors excused: Randy Richardson

Others present:

Debra Thatcher	Natalya Brown	April Hamlin	Jessica Richardson
Robynne Wilgus	Steve Rogers	Cathy Chapman	Kelley Plueard

Citizen comments: There were none.

Changes to the agenda: Board Policy 2432 will be pulled from the consent agenda and discussed under Old Business. A discussion on refinancing the Lang Center will be added under New Business.

Consent Agenda:

1. Minutes of College Board Meeting of February 12, 2020
2. Minutes of College Special Board Meeting of February 26, 2020
3. Personnel Actions
4. The following policies were presented to the Board for a second reading:

<u>Old #</u>	<u>New #</u>	<u>Title</u>
600.4	3310	Records, Retention and Destruction
404	3440	Animals on Campus
N/A	5200	Student Health Services (No AP)
N/A	5210	Communicable Disease – Students
N/A	5400	Associated Students Organization
N/A	5410	Associated Students Elections
N/A	5420	Associated Students Finance
740	5610	Voter Registration & Information
600.05	6300	Fiscal Management
N/A	6316	Debt Issuance and Management
601	6330	Purchasing

<u>OLD</u>	<u>NEW</u>	<u>TITLE</u>
100	2000	Organization and Authority
100.01	2010	Board of Education Membership
100.03	2100	Board of Education Elections
100.05	2110	Vacancies on the Board of Education
100.05	2110AP	Vacancies on the Board of Education
100.1	2200	Board of Education Duties and Responsibilities
100.04, .11, .12, .13	2210	Board of Education Officers

OLD	NEW	TITLE
100.06	2220	Committees of the Board of Education
N/A	2305	Board of Education Annual Organizational Meeting
103	2310	Regular Meetings of the Board of Education
103.01	2310AP	Regular Meetings
103.02	2315	Closed Executive Sessions
103.03	2320	Special Meetings
103.03, .04	2320AP	Special and Emergency Meetings
103AP	2330	Quorum and Voting
103.05	2340	Agendas
103.05AP	2345	Public Participation at Board of Education Meetings
103AP	2350	Speakers
103AP	2355	Decorum
103.06	2360	Minutes
101, 101.01, 102	2410	Board Policies and Administrative Procedures
100.07, 14	2430	Delegation of Authority to the President
N/A	2431	Selection of the President
N/A	2435	Evaluation of the President
N/A	2610	Presentation of Initial Collective Bargaining Proposals
N/A	2610AP	Presentation of Initial Collective Bargaining Proposals
104	2710	Conflict of Interest
104	2710AP	Conflict of Interest
100.08	2715	Code of Ethics / Standards of Practice
N/A	2716	Board of Education Political Activity
N/A	2717	Personal Use of Public Resources - Board of Education
100.07	2720	Communications Among Board of Education Members
100.09	2725	Board of Education Member Compensation
N/A	2735	Board of Education Member Travel
100.17	2745	Board of Education Self Evaluation
107	2800	Separation of College and Foundation

The following policies were presented to the Board for a second reading for deletion:

#	Title
100.15	Legal Counsel
106	Association Memberships

The Consent Agenda was approved by general consent; the items are attached to the permanent minutes.

STANDING REPORTS

- **ASUCC, ACEUCC, UCCFA, AND UCCPTFA:** No report
- **OCCA – Dir. Lathrop:** Copies of the OCCA End of Session Legislative Report 2020 were shared.
- **President – Dr. Thatcher:** The written report will be attached to the permanent meeting minutes. Topics reviewed were COVID-10 preparation, Strategic Plan, Accreditation, Safety lockdown drills, Enrollment, Resource allocation, and Academic restructuring.
- **Chair – Chair Loosley:** No report.

INFORMATIONAL REPORTS

- Accreditation – President Thatcher shared that Emily Fiocco has taken another position in the community and will work part time for UCC through September. The college is on track for continuity in accreditation.
- Advancement and Enrollment submitted written reports.

OLD BUSINESS

Policy 2432 Designation of Acting President, which was pulled from the Consent Agenda, will be revised and returned to the Board for review.

NEW BUSINESS

Natalya Brown, Chief Financial Officer, introduced the option of refinancing of the Full Faith and Credit Obligations 2010. June 1 is the deadline for calling an exemption. It will take about three months to finalize. After a brief discussion, it was suggested to have a Special Board meeting in the morning of March 17 for further information.

President Thatcher presented policies for a first reading; there were no questions.

Old #	New #	Title
N/A	4010	Academic Calendar
344	4030	Academic Freedom
N/A	4106	Nursing Programs
600.08	5800	Prevention of Identity Theft in Student Financial Transactions

Chair Loosley led a discussion regarding a possible bond capital campaign to fund college improvements. The projects would possibly be a new Industrial Technology Center, remodeling of Lockwood Hall, and deferred maintenance. President Thatcher stressed the importance of having current facilities to meet training needs. At next month's work session, the focus will be on the use of space, cost, and hearing from the people in the related instructional programs.

Board Comments: There were none.

Meeting adjourned at 6:36 p.m.

Respectfully submitted,

Approved,

Debra H. Thatcher, Ph.D.
 Clerk of the Board

Steve Loosley
 Chair of the Board

Recorded by Robynne Wilgus

Attachments to Permanent Minutes: Personnel Actions; Policies: 2nd Reading: 100.15, 106, 2000, 2010, 2100, 2110, 2200, 2210, 2220, 2305, 2310, 2315, 2320, 2330, 2340, 2345, 2350, 2355, 2360, 2410, 2430, 2431, 2435, 2610, 2710, 2715, 2716, 2717, 2720, 2725, 2735, 2745, 2800, 3310, 3440, 5200, 5210, 5400, 5410, 5420, 5610, 6300, 6316, 6330; 1st Reading: 4010, 4030, 4106, 5800; President's Report

**UMPQUA COMMUNITY COLLEGE
BUDGET COMMITTEE MINUTES**

On Thursday, March 12, 2020, the Umpqua Community College Budget Committee met on campus in Room 15 of Tap^hòyt^ha' in Roseburg, Oregon. The meeting was called to order at 6:00 p.m. by Sally Dunn, 2019 Chair, and the pledge of allegiance was given.

Budget Directors Present: Sally Dunn, Matt Fullerton, Hop Jackson, Sandy Henry, Joelle McGrorty, Rex Stevens, Steve Loosley, Guy Kennerly, Twila McDonald, David Littlejohn, Erica Mills, Doris Lathrop, and Randy Richardson

Budget Director Excused: Tom Davidson

Others Present: Debra Thatcher, Robynne Wilgus, Natalya Brown, Katie Workman, and Tim Hill

Changes to the Agenda: There were none.

Organization for 2020-2021:

Chair: Chair Loosley nominated BC Dunn, Dir. Jackson seconded the nomination and a unanimous vote was cast. BC Dunn accepted the nomination and said she has been on the committee through nine presidents; she encouraged younger people to be engaged in the process.

Vice Chair: Chair Loosley nominated Dir. Lathrop, BC Stevens seconded the nomination and a unanimous vote was cast.

Secretary: Chair Loosley nominated Dir. McDonald, BC Jackson seconded the nomination and a unanimous vote was cast.

Motion: **I move for an adjournment time of 8:30 p.m. Motion by BC Stevens, seconded by BC Fullerton and carried unanimously.**

President's Message

The College went through a new process of aligning resource allocation with accreditation. Positions and activities that are one-time or sustainable and contribute to the priorities of enrollment or compliance have been funded by shifting monies.

Natalya Brown, Chief Financial Officer, reviewed the duties of the Budget Committee which include: receiving the budget message, providing an opportunity for the public to comment on the budget, approving the budget, and approving the tax rate. The budget timeline and process was reviewed.

Budget principles were shared:

1. Ensure the College's strategic priorities and mission is fulfilled.
2. Consider investment and reduction decisions through the College's values of: knowledge, sense of community, integrity, and improvement and innovation.
3. Maintain: student success, enrollment, and retention; staffing and services at sufficient levels; sufficient fund balance; flexibility; and a balanced budget.
4. Invest in initiatives, strategies, programs, and operations that will positively impact student completion and success.
5. Seek cost-sharing and revenue-producing opportunities that support the College's mission and strategic priorities.

The strategic budget allocation process is a new college-wide method used to support strategic directions. The resource requests went through two rounds of review using fiscal impact/sustainability, student success, enrollment, and compliance criteria. The allocation summary was reviewed.

The budget structure combines 10 different funds: General, Capital Projects, Special Revenue, Administratively Restricted, Insurance, Enterprise, Financial Aid, Agency, Debt Services, and Internal Service. A summary of the proposed budget for the funds was reviewed.

General Fund

- Highlights: Through academic restructuring and shifting current funds, the College was able to fund several full-time and part-time positions. Many cost centers were combined to increase operating efficiencies.
- Revenue Sources: state allocation; tuition and fees; and property taxes.
- Assumptions:
 - State funding for community colleges: During the 2019-21 biennium, \$640.9 million will come from the state; this is \$6.1 million short from the collective ask to retain current service level funding.
 - Tuition and Fees: A 5% decrease in enrollment is projected. Tuition has increased by \$3 per credit and there are proposed fee increases.
 - Property taxes: A 2% rate of growth is projected.

Ms. Brown reviewed the budget changes in revenue, compared UCC tuition with other community colleges, and showed a graph chart of general fund resources since 2008-09. The largest change in budget requirements is the increase to employee salaries and benefits. The general fund operating requirement description was reviewed. Labor and Fringe is budgeted for the full year; savings is obtained during that time through vacancies and personnel changes. A 10-year history of Labor and Fringe data was reviewed. The operating contingency was explained. Reserves cannot be touched; they provide financial stability. The ending fund balance of \$6,033,893 meets the Board policy target of 18%. Discussion included the realization of increased labor costs amid shrinking enrollment. The College doesn't spend all of what is budgeted.

Resources and requirements were reviewed for the following funds:

Grants & Contracts: The fund is for the proceeds of revenue sources that are legally restricted to expenditures for special purposes. Examples: federal, state, and local grants and contracts.

Special Revenue: The fund accounts for activities that supplement the regular general fund programs and are intended to be self-supporting in nature. The main revenue is from fees or revenue-generating activities.

Financial Aid: This is a pass-through fund from federal, state, and local sources. The College receives the funds and then distributes them to students.

Capital Projects: The account is for capital projects, deferred maintenance, furnishing and equipment, and pool repairs. The revenue source is through a transfer from the general fund. The large project for the upcoming year is planning and preparation for the Industrial Technology Center; \$150,000 has been budgeted for the related expenses.

Debt Service: General fund transfer and Legacy Fees provide the resources for the repayment of obligations for PERS bonds and Full Faith and Credit Obligations (FFCO) 2010 and 2014. FFCO 2014 Series A were paid in full in FY20.

Insurance: A transfer from the general fund provides resources for self-funded unemployment insurance and early retirement health insurance provided to employees meeting specific service criteria requirements.

Enterprise: The fund is for the Campus Store, Incubator, Special Events, and Wine Sales programs. Food Services has been absorbed into the Campus Store operations. The deficit in the Catering fund is being covered by the College in the next couple of years with a transfer.

Internal Service: The fund is comprised of three cost centers – motor pool, copiers, and PERS reserves. A new copier lease agreement is being negotiated with the hope of reducing costs.

Agency: The activities of student government (ASUCC) and student clubs are handled through this fund. Revenue is derived from student club activities, a general fund transfer, and student activity fees which are transferred from the administratively restricted fund.

After a brief meeting break, BC Dunn clarified the total budget amount, \$54,199,497, on page 18 of the budget document doesn't include the unappropriated and reserve amounts. The full amount of \$61,772,147 will be stated during the motion for approval.

Citizen Comments – There were none.

Motion: I move that the budget committee of Umpqua Community College approve the budget for the 2020-2021 fiscal year in the amount of \$61,772,147. Motion by Chair Loosley and seconded by BC Stevens. The motion was unanimously approved.

Motion: I move that the budget committee of Umpqua Community College approve property taxes for the 2020-21 fiscal year at the rate of \$0.4551 per \$1,000 of assessed value for the permanent rate tax levy. Motion by Chair Loosley and seconded by Dir. Lathrop. The motion was unanimously approved.

Ms. Brown thanked the Budget Committee members for their service.

Meeting adjourned at 7:19 p.m.

Respectfully submitted,

Approved,

Twila McDonald
Secretary

Sally Dunn
Chair

Recorded by Robynne Wilgus

UMPQUA COMMUNITY COLLEGE
BOARD MINUTES
March 17, 2020

The Umpqua Community College Board of Education met for a Special Meeting on Tuesday, March 17, 2020, via Zoom conference connection. Board Chair Loosley called the meeting to order at 8:34 a.m.

Directors present: Guy Kennerly, Doris Lathrop, David Littlejohn, Twila McDonald, Erica Mills, Randy Richardson, and Steve Loosley

Others present: Debra Thatcher, Robynne Wilgus, Natalya Brown, and Matt Donahue

Changes to the agenda: None

OLD BUSINESS

Natalya Brown, Chief Financial Officer, requested Board approval to authorize the issuance of a full faith and credit financing agreement (the "Financing Agreement") to refund the Refundable Obligations and pay costs of issuance. The Financing Agreement shall be sold and issued as provided in this Resolution and pursuant to ORS Chapter 287A and ORS 271.390. The Financing Agreement shall be issued in an amount necessary to refund the Refundable Obligations and to pay costs of issuance. The District finds that the refunding is needed and that the estimated weighted average life of the Financing Agreement will not exceed the dollar weighted average life of the projects being refinanced with the Financing Agreement, as required by ORS 271.390.

Matt Donahue, from D.A. Davidson, shared what happens under normal market conditions while recognizing the current market is not normal. The savings in purchasing new tax-exempt bonds was explained. The full process takes about 6-8 weeks and not out of pocket cash contribution is needed.

Resolution No. 13:

Authorizing the Refunding of the District's Series 2010 Obligations and Paying Costs of Issuance

MOTION: I move to approve the authorization of Res. No. 13, refunding the district's series 2010 obligations and paying costs of issuance, as presented. Motion by Chair Loosley, seconded by Dir. Littlejohn and carried unanimously.

Chair Loosley introduced Resolution No. 14, declaring emergency conditions exist at the College and granting authority to take any and all necessary actions to prepare and respond effectively to the novel coronavirus (COVID-19). President Thatcher explained it allows the College to operate differently, such as in procurement matters. In Board discussion concern was expressed, due to many unknowns, including federal and state programs to care for and support workers who were laid off because of the virus. Ms. Brown confirmed the College is tracking all expenses connected to COVID-19 in case FEMA or other federal funding becomes available. The Board approved a revised resolution without the second clauses about pay.

Resolution No. 14: Declaring Emergency Conditions

MOTION: I move to approve Res, No. 14, declaring emergency conditions, as presented. Motion by Dir. Littlejohn and seconded by Dir. Kennerly. The motion was approved by Chair Loosley and Directors Kennerly, Lathrop, Littlejohn, McDonald, and Richardson. (Dir. Mills left the meeting prior to the vote.)

Meeting adjourned at 9:29 a.m.

Respectfully submitted,

Approved,

Debra H. Thatcher, Ph.D.
Clerk of the Board

Steve Loosley
Chair of the Board

Recorded by Robynne Wilgus

Attachments to Permanent Minutes: Resolutions 13 & 14

Please note: There was an error in the posted meeting time on the agenda. The agenda indicated Noon; the meeting actually began about 8:30 a.m. Media contacts were notified and a recording was sent out as requested.



Serving Douglas County Since 1964

TO: UCC Board of Education
FROM: Kelley Plueard, Director of Human Resources
SUBJECT: Personnel Actions
DATE: April 8, 2020

Board approval is requested on the following personnel actions:

Administrative Contracts:

Kimberly Meinhardt, Director of SSS TOP - Effective April 6, 2020

Robin Van Winkle, Dean of Community Education and Partnerships - Effective March 30, 2020

Faculty Contracts:

N/A

Resignations/Separations:

Elizabeth Bastian, Director of Grant Development – Effective April 15, 2020



BOARD POLICY

TITLE: DESIGNATION OF ACTING PRESIDENT

BOARD POLICY # 2432

Should the President not be able to perform the duties of his/her position for short periods of time, the duties of the President will automatically be delegated by the Board to the Chief Academic Officer, or if that College administrator is not able to assume the President's duties, to the Chief Financial Officer.

The Board shall appoint an Acting President if the President's inability to perform his/her duties is expected to exceed five working days. The Board will generally appoint a senior level administrator as Acting President, giving the Chief Academic Officer and the Chief Financial Officer first consideration for such an appointment.

The Board's appointment of an Acting President will generally not exceed 30 calendar days at a time; however, the Board of Education shall have the option to appoint an Acting President for periods exceeding 30 calendar days.

RESPONSIBILITY:

The Board Chair is responsible for implementing and updating this policy.

NEXT REVIEW DATE:

DATE OF ADOPTION:

DATE(S) OF REVISION:

DATE(S) OF PRIOR REVIEW:



BOARD POLICY

TITLE: Academic Calendar

BOARD POLICY # 4010

The Chief Academic Officer shall, in consultation with the appropriate groups and following the college-wide shared governance process, develop an academic calendar. The proposed calendar will be submitted to the Board of Education for approval.

RESPONSIBILITY:

The Chief Academic Officer is responsible for implementing and updating this policy. Specific guidance for policy implementation may be found in the associated Administrative Procedure(s).

NEXT REVIEW DATE:

DATE OF ADOPTION:

DATE(S) OF REVISION:

DATE(S) OF PRIOR REVIEW:

POLICY / ADMINISTRATIVE PROCEDURE CONVERSION TEMPLATE

Complete for Conversions Only

<p>TITLE: Academic Calendar</p> <p>New BP #: 4010 Old BP # & Title: 707 Academic Calendar</p> <p>New AP #: Old AP # & Title:</p> <p>Revision Date: 4/10/2019</p>
--

EXISTING POLICY / PROCEDURE	OCCA POLICY / PROCEDURE	PROPOSED POLICY / PROCEDURE
<p>The Vice President of Instruction will establish an annual academic calendar in conjunction with a college-wide shared governance process. After the calendar has been approved by the Board, it will be posted on the UCC website.</p>	<p>The [CEO] shall, in consultation with the appropriate groups, [develop or submit to the Board of Education for approval] an academic calendar.</p>	<p>The Chief Academic Officer shall, in consultation with the appropriate groups and following the college-wide shared governance process, develop an academic calendar. The proposed calendar will be submitted to the Board of Education for approval.</p>



ADMINISTRATIVE PROCEDURE

TITLE: ACADEMIC CALENDAR

ADMINISTRATIVE PROCEDURE # 4010

RELATED TO POLICY # 4010 Academic Calendar

A. The College's three-year academic calendar shall include , at minimum, the following:

1. class registration
2. payment deadlines
3. dates classes begin and end each term (summer, fall, winter, and spring)
4. final examinations
5. last date to drop class(es) and be eligible for a refund as well as to add, withdraw, and/or change status from credit to audit
6. exceptions to the above for classes that meet for shorter periods during the term
7. college holidays, spring break, winter break, and campus closings
8. petition to graduate deadlines
9. Commencement

B. The academic calendar shall be of sufficient length to ensure the equivalent of 11 weeks of instruction per term (including final examination days) for all credit classes.

C. The Director of Registration and Records and the Chief Academic Officer will make reasonable efforts to coordinate the College's academic calendar with those of the public schools and regional institutions of higher education so that start dates and class breaks of any appreciable length (such as annual spring break) coincide in most systems.

D. After vetting through the appropriate College entities and approval by the College Board of Education for approval, the approved three-year calendar is published in the website. The UCC website will also post tentative academic calendars for the next two years.

RESPONSIBILITY:

The Chief Academic Officer is responsible for implementing and updating this procedure.

NEXT REVIEW DATE:

DATE OF ADOPTION:

DATE(S) OF REVISION:

DATE(S) OF PRIOR REVIEW:

POLICY / ADMINISTRATIVE PROCEDURE CONVERSION TEMPLATE

Complete for Conversions Only

TITLE: Academic Calendar New BP #: Old BP # & Title: New AP #: 4010 Old AP # & Title: Revision Date: 4/10/2019

EXISTING POLICY / PROCEDURE	OCCA POLICY / PROCEDURE	PROPOSED POLICY / PROCEDURE
NA	<ul style="list-style-type: none"> The number of days that define an academic year Flexible calendar options, if any Processes for determining the academic calendar Holidays, which include: [<i>insert</i>] <p>Other Holidays – The Board of Education may declare other days to be holidays and close the colleges and offices when good reason exists.</p> <p>NOTE: <i>These holidays may include New Year's Eve day, the day after Thanksgiving, and Christmas Eve day.</i></p>	<p>The college's academic calendar shall include the dates of all operational activities that affect students and the public (such as registration dates and holidays during which the college is closed). These dates shall include, but not be limited to, the following:</p> <ul style="list-style-type: none"> class registration graduation ceremony midterm and final examinations college holidays, and campus closings petition to graduate deadlines beginning and ending of summer, fall, winter, and spring quarters return dates for full-time faculty dates classes begin and end each term last date to drop class(es) and be eligible for a refund as well as to add, withdraw, and/or change status from credit to audit payment deadlines.

		<p>The academic calendar should be of sufficient length to insure the equivalent of 11 weeks of instruction per term (including final examination days) for all credit classes.</p> <p>The Registrar and the Chief Academic Officer will make reasonable efforts to coordinate the college's academic calendar with that of the public schools and regional institutions of higher education so that start dates and class breaks of any appreciable length (such as annual spring break) coincide in most systems.</p> <p>After vetting through the appropriate UCC entities, the proposed academic calendar is submitted to the UCC board of education for approval, and the approved calendar is published in the college catalog, schedule and website. The UCC website will also post tentative academic calendars for the next two years.</p>
--	--	---



BOARD POLICY

TITLE: Academic Freedom

BOARD POLICY # 4030 *was 344 Academic Freedom*

Umpqua Community College is committed to the principle that institutions of higher learning benefit from academic freedom. Umpqua Community College defines academic freedom as the faculty's right to engage in intellectual debate, research, speech, writing, artistic expression, and all other forms of communication, both on and off campus, without fear of censorship or reprisal.

RESPONSIBILITY:

The Chief Academic Officer is responsible for implementing and updating this policy. Specific guidance for policy implementation may be found in the associated Administrative Procedure(s).

NEXT REVIEW DATE:

DATE OF ADOPTION:

DATE(S) OF REVISION:

DATE(S) OF PRIOR REVIEW:

POLICY / ADMINISTRATIVE PROCEDURE CONVERSION TEMPLATE

Complete for Conversions Only

TITLE: Academic Freedom
New BP #: 4030 Old BP # & Title: 344 Academic Freedom
New AP #: Old AP # & Title:
Revision Date: 4/10/2019

EXISTING POLICY / PROCEDURE	OCCA POLICY / PROCEDURE	PROPOSED POLICY / PROCEDURE
<p>Umpqua Community College is committed to the principle that institutions of higher learning benefit from academic freedom. Umpqua Community College defines academic freedom as the faculty's right to engage in intellectual debate, research, speech, writing, artistic expression, and all other forms of communication, both on and off campus, without fear of censorship or reprisal.</p>	<p>The [entity] shall support the principles of academic freedom, built upon the free expression and exchange of ideas that are inherent in the search for scholarly truth and upon which a free and democratic society depends. The College affirms the use of a variety of teaching methodologies to fulfill its obligation to raise difficult and meaningful questions in the educational development of students. Faculty members are entitled to freely discuss issues germane to their subject matter. This freedom involves the right to introduce controversial topics, as long as the manner of presentation involves objective reasoning and rational discussion.</p> <p>Academic freedom must be balanced with the obligation of the College to protect the right of students to learn in an environment characterized by civility, open inquiry, and</p>	<p>Umpqua Community College is committed to the principle that institutions of higher learning benefit from academic freedom. Umpqua Community College defines academic freedom as the faculty's right to engage in intellectual debate, research, speech, writing, artistic expression, and all other forms of communication, both on and off campus, without fear of censorship or reprisal.</p>

	<p>freedom from unlawful discrimination. While faculty have the right to present ideas and conclusions which they believe to be in accord with available evidence, they also have the responsibility to acknowledge the existence of different opinions and to respect the right of others to hold those views. Faculty and students have a responsibility to engage in teaching and learning that honors and respects divergent viewpoints that are grounded in cultures of reason, logic, evidence and responsible scholarship.</p> <p>When faculty (or any other College employees) speak or write as citizens, care should be taken to avoid the representation of any personal view as that of the [entity].</p>	
--	--	--



ADMINISTRATIVE PROCEDURE

TITLE: Academic Freedom

ADMINISTRATIVE PROCEDURE # 4030

RELATED TO POLICY # 4030 Academic Freedom

Academic Freedom includes the following rights and responsibilities:

- A. Faculty are entitled to freedom in the classroom in discussion and presentation of subject matter, both online and face-to-face. This includes the right to explore and discuss controversial issues and divergent points of view in relationship to the subject matters being discussed.
- B. When speaking or writing as private individuals, faculty are entitled to exercise all rights of citizenship, as defined by and in accordance with decisions of the state and federal courts, and are free from institutional censorship or discipline. As scholars and educational officers, they should remember that the public may judge their profession and their institution by their statements. Therefore, in their written statements and at public speaking events, faculty should not state they are speaking for the institution.
- C. Faculty are entitled to full freedom in intellectual inquiry and expression in terms of research, speech, writing, artistic endeavors, and all other forms of communication related to their discipline.
- D. Any faculty who feels their rights have been violated in regards to Academic Freedom should refer to the grievance procedure outlined in their respective bargaining agreements.

References: NWCCU Standards 2.A.27 and 2.A.28; OAR 589-008-0100(f)

RESPONSIBILITY:

The Chief Academic Officer is responsible for implementing and updating this procedure.

NEXT REVIEW DATE:

DATE OF ADOPTION:

DATE(S) OF REVISION:

DATE(S) OF PRIOR REVIEW:

POLICY / ADMINISTRATIVE PROCEDURE CONVERSION TEMPLATE

Complete for Conversions Only

TITLE: Academic Freedom New BP #: Old BP # & Title: New AP #: 4030 Old AP # & Title: 344 AP Academic Freedom Revision Date: 10/17/2019

EXISTING POLICY / PROCEDURE	OCCA POLICY / PROCEDURE	PROPOSED POLICY / PROCEDURE
N/A	<p>References: NWCCU Standards 2.A.27 and 2.A.28 OAR 589-008-0100(f)</p> <p>NOTE: <i>Although this policy is recommended as good practice, it is up to the entity to determine the applicability of this administrative procedure given state law and the entity's organizational culture. Local practice may be inserted here to implement board policy, if necessary.</i></p> <p>NOTE: Oregon administrative rules address the formation of community college personnel policies by Boards of Education. OAR 589-008-0100(f) requires a statement regarding academic freedom and responsibilities. BP 4030 provides sample language and any additional language related to procedures may be added here.</p>	<p>Academic Freedom includes the following rights and responsibilities:</p> <ul style="list-style-type: none"> A. Faculty are entitled to freedom in the classroom in discussion and presentation of subject matter, both online and face-to-face. This includes the right to explore and discuss controversial issues and divergent points of view in relationship to the subject matters being discussed. B. When speaking or writing as private individuals, faculty are entitled to exercise all rights of citizenship, as defined by and in accordance with decisions of the state and federal courts, and are free from institutional censorship or discipline. As scholars and educational officers, they should remember that the public may judge their profession and their institution by their statements. Therefore, in their written statements and at public speaking events, faculty should not state they are speaking for the institution. C. Faculty are entitled to full freedom in intellectual inquiry and expression in terms of research, speech, writing, artistic endeavors, and all other forms of communication related to their discipline.

		<p>D. Any faculty who feels their rights have been violated in regards to Academic Freedom should refer to the grievance procedure outlined in their respective bargaining agreements.</p>
--	--	--



BOARD POLICY

TITLE: Nursing Programs

BOARD POLICY # 4106

The UCC nursing programs will adhere to all applicable regulations, laws, and requirements located in Oregon ORS and OAR, as well as standards of all applicable accrediting or approval bodies, such as Oregon State Board of Nursing.

UCC nursing programs will maintain a detailed student code of conduct applicable to any student admitted to the nursing program. If a conflict exists with the UCC Student Code of Conduct, the nursing program code of conduct will prevail.

RESPONSIBILITY:

The Chief Academic Officer is responsible for implementing and updating this policy. Specific guidance for policy implementation may be found in the associated Administrative Procedure(s).

NEXT REVIEW DATE:

DATE OF ADOPTION:

DATE(S) OF REVISION:

DATE(S) OF PRIOR REVIEW:



ADMINISTRATIVE PROCEDURE

TITLE: Nursing Programs

ADMINISTRATIVE PROCEDURE # 4106

RELATED TO POLICY # 4106 Nursing Programs

- A. The College's Associate Degree of Nursing (ADN) Program shall comply with relevant laws (ORS 678.010-678.445) and rules (OAR 851 Division 21) of the Oregon Nurse Practice Act.
- B. Requirements of the relevant laws and rules include, but are not limited to:
1. Written program policies and procedures, congruent with those of the College, which are reviewed periodically.
 2. Faculty responsibilities:
 - a. Develop, implement and evaluate policies and standards for the advising, selection, admission, advanced placement, progression and graduation of nursing students within the framework of the policies of the College
 - b. Develop, implement and evaluate policies for assessing student achievement in terms of course and program learning outcomes
 - c. Evaluate student learning and performance, assign grades for courses according to policies, determine student progression within the program, and recommend successful candidates for the ADN degree
 - d. Develop, implement and evaluate policies and procedures necessary for the operation of the ADN program
 - e. Participate in review of the total nursing program
 - f. Participate in determining academic policies and procedures of the College
 - g. Provide mechanisms for student input into and/or participation in decisions related to the ADN Program
 3. Written information for students regarding admission, readmission, transfer, progression, retention, dismissal and graduation requirements that are consistent with those of the College along with policies, procedures, and

processes specific to nursing students if justified by the nature and purposes of the ADN Program.

4. Biennial review of program policies and procedures to assure compliance with the OSBN Nurse Practice Act, Division 21 Rules.

C. The UCC ADN Policy Manual will be reviewed every two years.

D. The UCC ADN Student Procedures Handbook will be reviewed annually (each spring term).

References

ORS 678.010-678.445 Oregon Nurse Practice Act
OAR 851

RESPONSIBILITY:

The Chief Academic Officer, in conjunction with the Director of Nursing, is responsible for implementing and updating this procedure.

NEXT REVIEW DATE:

DATE OF ADOPTION:

DATE(S) OF REVISION:

DATE(S) OF PRIOR REVIEW:



BOARD POLICY

TITLE: PREVENTION OF IDENTITY THEFT IN STUDENT FINANCIAL TRANSACTIONS

BOARD POLICY # 5800 *(was 600.08 Identity Theft Prevention)*

The College is required to provide for the identification, detection, and response to patterns, practices, or specific activities (“Red Flags”) that could indicate identity theft of students when the College serves as a creditor in relation to its students. When applicable, the Chief Financial Officer is directed to develop procedures to implement an Identity Theft Prevention Program (ITPP) to control reasonably foreseeable risks to students from identity theft.

References:

15 U.S. Code Section 1681m(e), (Fair and Accurate Credit Transactions Act)

ORS 646A.600 to 646A.628 (Oregon Consumer Identity Theft Protection Act)

RESPONSIBILITY:

The Chief Financial Officer is responsible for implementing and updating this policy. Specific guidance for policy implementation may be found in the associated Administrative Procedure(s).

NEXT REVIEW DATE:

DATE OF ADOPTION:

DATE(S) OF REVISION:

DATE(S) OF PRIOR REVIEW:

POLICY / ADMINISTRATIVE PROCEDURE CONVERSION TEMPLATE

Complete for Conversions Only

TITLE: Prevention of Identity Theft in Student Financial Transactions New BP #: 5800 Old BP # & Title: 600.08 Identity Theft Prevention New AP #: Old AP # & Title: Revision Date: 11/15/2019
--

EXISTING POLICY / PROCEDURE	OCCA POLICY / PROCEDURE	PROPOSED POLICY / PROCEDURE
<p>To prevent identity theft, the Board of Education of Umpqua Community College directs the College to comply with the Federal Trade Commission "Red Flag Rule" which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 by maintaining and monitoring this program.</p>	<p>References:</p> <p>15 U.S. Code Section 1681m(e), (Fair and Accurate Credit Transactions Act)</p> <p>ORS 646A.600 to 646A.628 (Oregon Consumer Identity Theft Protection Act)</p> <p style="background-color: yellow;">NOTE: This policy is legally required.</p> <p>The [entity] is required to provide for the identification, detection, and response to patterns, practices, or specific activities ("Red Flags") that could indicate identity theft of students</p>	<p>The College is required to provide for the identification, detection, and response to patterns, practices, or specific activities ("Red Flags") that could indicate identity theft of students when the College serves as a creditor in relation to its students. When applicable, the Chief Financial Officer is directed to develop procedures to implement an Identity Theft Prevention Program (ITPP) to control reasonably foreseeable risks to students from identity theft.</p> <p>References:</p> <p>15 U.S. Code Section 1681m(e), (Fair and Accurate Credit Transactions Act)</p> <p>ORS 646A.600 to 646A.628 (Oregon Consumer Identity Theft Protection Act)</p>

	<p>when the [entity] serves as a creditor in relation to its students. When applicable, the [CEO] is directed to develop procedures to implement an Identity Theft Prevention Program (ITPP) to control reasonably foreseeable risks to students from identity theft.</p>	<p>RESPONSIBILITY: The CFO is responsible for implementing and updating this policy. Specific guidance for policy implementation may be found in the associated Administrative Procedure(s).</p>
--	---	---



ADMINISTRATIVE PROCEDURE

TITLE: PREVENTION OF IDENTITY THEFT IN STUDENT FINANCIAL TRANSCATIONS

ADMINISTRATIVE PROCEDURE # 5800 *(was 600.08 Red Flag Rules)*

RELATED TO POLICY # 5800 PREVENTION OF IDENTITY THEFT

I. The Purpose of the Identity Theft Prevention Program

The purpose of this Identity Theft Prevention Program (ITPP) is to control reasonably foreseeable risks to students from identity theft, by providing for the identification, detection, and response to patterns, practices, or specific activities (“Red Flags”) that could indicate identity theft.

II. Definitions

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

- A. A “creditor” includes government entities who defer payment for goods (for example, payment plans for tuition payments or parking tickets), issued loans or issued student debit cards. Government entities that defer payment for services provided are not considered creditors for purposes of this ITPP.
- B. “Deferring payments” refers to postponing payments to a future date and/or installment payments on fines or costs.
- C. A “Covered Account” includes one that involves multiple payments or transactions.
- D. “Program Administrator” is the individual designated with primary responsibility for oversight of the program.
- E. “Person” means any individual who is receiving goods, receives a loan, and/or is issued a debit card from the College and is making payments on a deferred basis for said goods, loan, and/or debit card.
- F. “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.

- G. Detection or discovery of a “Red Flag” implicates the need to take action under this ITPP to help prevent, detect, and correct identity theft.

III. Detecting “Red Flags” For Potential Identity Theft

A. Risk Factors for Identifying “Red Flags”

The College will consider the following factors in identifying relevant “Red Flags:”

1. the types of covered accounts the College offers or maintains;
2. the methods the College provides to open the College’s covered accounts;
3. the methods the College provides to access the College’s covered accounts;
and
4. the College’s previous experience(s) with identity theft.

B. Sources of “Red Flags”

The College will continue to incorporate relevant “Red Flags” into this ITPP from the following sources:

1. incidents of identity theft that the College has experienced;
2. methods of identity theft that the College identifies that reflects changes in identity theft risks; and
3. guidance from the College’s staff who identify changes in identity theft risks.

C. Categories of “Red Flags”

The following Red Flags have been identified for the College’s covered accounts:

- 1. Alerts, Notifications, or Warnings from a Consumer Reporting Agency:**
 - a. A fraud or active duty alert is included with a consumer report the College receives as part of a background check.
 - b. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
 - c. A consumer reporting agency provides a notice of address discrepancy. An address discrepancy occurs when an address provided by a student or an employee substantially differs from the one the credit reporting agency has on file. See Section (V)(10) for specific steps that must be taken to address this situation.
 - d. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant, such as:

- 1) A recent and significant increase in the volume of inquiries;
- 2) An unusual number of recently established credit relationships;
- 3) A material change in the use of credit, especially with respect to recently established credit relationships; or
- 4) An account that was closed for cause or identified for abuse of account privileges by a creditor or financial institution.

2. Suspicious Documents:

- a. Documents provided for identification appear to have been forged or altered.
- b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- d. Other information on the identification is not consistent with readily accessible information that is on file with the College, such as a signature card or a recent check.
- e. An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

I. Suspicious Personally Identifying Information:

- a. Personal identifying information provided is inconsistent when compared against external information sources used by the College.

For example:

- 1) The address does not match any address in the consumer report; or
 - 2) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- b. Personal identifying information provided by a person is not consistent with other personal identifying information provided by the person. For example, there is a lack of correlation between the SSN range and date of birth.
 - c. Personal identifying information is associated with known fraudulent activity as indicated by internal or third-party sources use by the College. For example:
 - 1) The address on an application is the same as the address provided on a fraudulent application;

- 2) The phone number on an application is the same as the phone number provided on a fraudulent application;
 - d. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the College. For example:
 - 1) The address on an application is fictitious, a mail drop, or a prison; or
 - 2) The phone number is invalid, or is associated with a pager or answering service.
 - e. The SSN provided is the same as that submitted by other persons currently being served by the College.
 - 1) The address or telephone number provided is the same or similar to the account number or telephone number submitted by an unusually large number of other persons being served by the College.
 - 2) The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
 - 3) Personal identifying information provided is not consistent with personal identifying information that is on file with the College.
 - 4) The person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
- II. Unusual Use Of – Or Suspicious Activity Relating To – A Covered Account:**
- a. A new covered account is used in a manner that is commonly associated with known patterns of fraud patterns. For example, a person makes a first payment, but there are no subsequent payments made.
 - b. A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example, there is:
 - 1) Nonpayment when there is no history of late or missed payments; or
 - 2) A material change in electronic fund transfer patterns in connection with a payment.
 - c. A covered account that has been inactive for a reasonably lengthy period of time is suddenly used or active.
 - d. Mail sent to the person holding the covered account is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the person's covered account.

- e. The College is notified that the person is not receiving paper account statements.
- f. The College is notified of unauthorized transactions in connection with a person's covered account.

Notices From Customers/Persons, Victims of Identity Theft, Law Enforcement Authorities, or Other Businesses About Possible Identity Theft in Connection with Covered Accounts:

The College is notified by a person with a covered account, a victim of identity theft, a law enforcement authority, or any other person, that it has opened a fraudulent account for a person engaged in identity theft.

IV. Measures to Detect "Red Flags"

The College shall do the following to aid in the detection of "Red Flags:"

- A. When a new covered account is open, the College shall obtain identifying information about, and information verifying the identity of, the student or other person seeking to open a covered account. Two forms of identification shall be obtained (at least one of which must be a photo identification).

The following are examples of the types of valid identification that a person may provide to verify the identity of the person seeking to open the covered account: valid state-issued driver's license, valid state-issued identification card, current passport, a Social Security Card, current residential lease, or copy of a deed to the person's home or invoice/statement for property taxes.

- B. Persons with covered accounts who request a change in their personal information on file, such as a change of address, will have the requested changes verified by the College.

The person shall provide at least one written form of verification reflecting the requested changes to the personal information. For example, if an address change is requested, then documentation evidencing the new address shall be obtained. If a phone number change is requested, then documentation evidencing the new phone number, such as a phone bill, shall be obtained.

V. Preventing and Mitigating Identity Theft

One or more of the following measures, as deemed appropriate under the particular circumstances, shall be implemented to respond to "Red Flags" that are detected:

- A. Monitor the covered account for evidence of identity theft;
- B. Contact the person who holds the covered account;
- C. Change any passwords, security codes, or other security devices that permit access to a covered account;
- D. Reopen the covered account with a new account number;
- E. Not open a new covered account for the person;
- F. Close an existing covered account;
- G. Notify the Program Administrator for determination of the appropriate step(s) to take;
- H. Not attempt to collect on a covered account or not sell a covered account to a debt collector;
- I. Notifying law enforcement;
- J. Where a consumer reporting agency provides an address for a consumer that substantially differs from the address that the consumer provided, the College shall take the necessary steps to for a reasonable belief that the College knows the identity of the person for whom the College obtained a credit report, and reconcile the address of the consumer with the credit reporting agency, if the College establishes a continuing relationship with the consumer, and regularly, and in the course of business, provides information to the credit reporting agency; or
- K. Determine that no response is warranted under the particular circumstances.

VI. Protect Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect identifying information:

- A. Ensure that its website is secure or provide clear notice that the website is not secure;
- B. Ensure complete and secure destruction of paper documents and computer files containing account information when a decision has been made to no longer maintain such information;
- C. Ensure that office computers with access to Covered Account information are password protected;
- D. Avoid use of social security numbers;
- E. Ensure computer virus protection is up to date; and
- F. Require and keep only the kinds of information that are necessary for College purposes.

VII. Updating the ITPP

The College shall update this ITPP on an annual basis to reflect changes in risks to persons with covered accounts, or to reflect changes in risks to the safety and soundness of the College from identity theft, based on the following factors:

- A. The experiences of the College with identity theft;
- B. Changes in methods of identity theft;
 - 1. Changes in methods to detect, prevent and mitigate identity theft;
 - 2. Changes in the types of covered accounts that the College maintains;
 - 3. Changes in the business arrangements of the College, including service provider arrangements.

VIII. Methods for Administering the ITPP

Oversight of the ITPP

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee (“Committee”) for the College headed by a Program Administrator who may be CFO or his or her appointee. The remainder of the committee membership comprises administrative positions from the areas of Human Resources, Information Technology, and Student Services. The Program Administrator will be responsible for ensuring appropriate training of College 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.

Oversight by the Program Administrator shall include:

- A. Assigning specific responsibility for the ITPP’s implementation;
- B. Reviewing reports prepared by the staff regarding compliance of the ITPP; and
- C. Approving material changes to the ITPP as necessary to address changing identity theft risks.

IX. Reports

- A. In General** – Staff responsible for the development, implementation, and administration of this ITPP shall report to the Program Administrator on an annual basis.
- B. Contents of Report** – The report shall address material matters to the ITPP and evaluate the following issues: the effectiveness of the policies and procedures in

addressing the risk of identity theft in connection with opening new covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the ITPP.

- C. Oversight of Service Provider Arrangements** – Whenever the College engages a service provider to perform an activity in connection with one or more covered accounts the College shall take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. To that end, the College shall require our service contractors, by contract, to have policies and procedures to detect relevant “Red Flags” that may arise in the performance of the service provider's activities, and either report the “Red Flags” to the College, or to take appropriate steps to prevent or mitigate identity theft.

References:

15 U.S. Code Section 1681m(e) (Fair and Accurate Credit Transactions Act (FACT ACT or FACTA))

ORS 646A.604(8) (notice exception – Oregon Consumer Identity Theft Protection Act)

RESPONSIBILITY:

The CFO is responsible for implementing and updating this procedure.

NEXT REVIEW DATE:

DATE OF ADOPTION:

DATE(S) OF REVISION:

DATE(S) OF PRIOR REVIEW:

POLICY / ADMINISTRATIVE PROCEDURE CONVERSION TEMPLATE

Complete for Conversions Only

TITLE: Prevention of Identity Theft in Student Financial Transactions	
New BP #:	Old BP # & Title:
New AP #: 5800	Old AP # & Title: 600.08 Red Flag Rules
Revision Date:	11/15/2019

EXISTING POLICY / PROCEDURE	OCCA POLICY / PROCEDURE	PROPOSED POLICY / PROCEDURE
<p>II. DEFINITIONS AND PROGRAM</p> <p>A. Red Flags Rule Definitions Used in this Program</p> <p>“Identity Theft” is a “fraud committed or attempted using the identifying information of another person without authority.”</p> <p>A “Red Flag” is a “pattern, practice, or specific activity that indicates the possible existence of Identity Theft.”</p> <p>A “Covered Account” includes all accounts that permit multiple transactions or poses a reasonable foreseeable risk of being used to promote identity theft.</p> <p>“Program Administrator” is the individual designated with primary responsibility for oversight of the program. See Section VI below.</p>	<p>Reference:</p> <p>15 U.S. Code Section 1681m(e) (Fair and Accurate Credit Transactions Act (FACT ACT or FACTA))</p> <p>ORS 646A.604(8) (notice exception – Oregon Consumer Identity Theft Protection Act)</p> <p>NOTE: <i>This procedure is legally required.</i></p> <p>I. The Purpose of the Identity Theft Prevention Program</p> <p>The purpose of this Identity Theft Prevention Program (ITPP) is to control reasonably foreseeable risks to students from identity theft, by providing for the identification, detection, and response to patterns,</p>	<p>I. The Purpose of the Identity Theft Prevention Program</p> <p>The purpose of this Identity Theft Prevention Program (ITPP) is to control reasonably foreseeable risks to students from identity theft, by providing for the identification, detection, and response to patterns, practices, or specific activities (“Red Flags”) that could indicate identity theft.</p> <p>II. Definitions</p> <p>“Identity theft” is a fraud attempted or committed using identifying information of another person without authority.</p> <p>A “creditor” includes government entities who defer payment for goods</p>

<p>“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.</p> <p>B. Fulfilling Requirements of the Red Flags Rule</p> <p>Under the Red Flags Rule, the College is required to establish an “Identity Theft Prevention Program” tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:</p> <ol style="list-style-type: none"> 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 	<p>practices, or specific activities (“Red Flags”) that could indicate identity theft.</p> <p>II. Definitions</p> <p>“Identity theft” is a fraud attempted or committed using identifying information of another person without authority.</p> <p>A “creditor” includes government entities who defer payment for goods (for example, payment plans for bookstore accounts or parking tickets), issued loans or issued student debit cards. Government entities that defer payment for services provided are not considered creditors for purposes of this ITPP.</p> <p>“Deferring payments” refers to postponing payments to a future date and/or installment payments on fines or costs.</p> <p>A “covered account” includes one that involves multiple payments or transactions.</p> <p>“Person” means any individual who is receiving goods, receives a loan, and/or is issued a debit card from the [entity] and is making payments on a deferred basis for said goods, loan, and/or debit card.</p> <p>Detection or discovery of a “Red Flag” implicates the need to take action</p>	<p>(for example, payment plans for tuition payments or parking tickets), issued loans or issued student debit cards. Government entities that defer payment for services provided are not considered creditors for purposes of this ITPP.</p> <p>“Deferring payments” refers to postponing payments to a future date and/or installment payments on fines or costs.</p> <p>A “Covered Account” includes one that involves multiple payments or transactions.</p> <p>“Program Administrator” is the individual designated with primary responsibility for oversight of the program.</p> <p>“Person” means any individual who is receiving goods, receives a loan, and/or is issued a debit card from the College and is making payments on a deferred basis for said goods, loan, and/or debit card.</p> <p>“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</p>
---	--	--

<p>to students, employees or other persons, or their safety and soundness from Identity Theft.</p> <p>III. IDENTIFICATION OF RED FLAGS In order to identify relevant Red Flags, the College considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. The College identifies the following Red Flags in each of the listed categories:</p> <p>A. Notifications and Warnings from Credit Reporting Agencies Red Flags</p> <ol style="list-style-type: none"> 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. <p>B. Suspicious Documents</p>	<p>under this ITPP to help prevent, detect, and correct identity theft.</p> <p>III. Detecting “Red Flags” For Potential Identity Theft</p> <p>A. Risk Factors for Identifying “Red Flags” The [entity] will consider the following factors in identifying relevant “Red Flags:”</p> <ol style="list-style-type: none"> 1) the types of covered accounts the [entity] offers or maintains; 2) the methods the [entity] provides to open the [entity's] covered accounts; 3) the methods the [entity] provides to access the [entity's] covered accounts; and 4) the [entity]s previous experience(s) with identity theft. <p>B. Sources of “Red Flags” The [entity] will continue to incorporate relevant “Red Flags” into this ITPP from the following sources:</p> <ol style="list-style-type: none"> 1) incidents of identity theft that the [entity] has experienced; 2) methods of identity theft that the [entity] identifies that reflects changes in identity theft risks; and 	<p>taxpayer identification number, student identification number, computer's Internet Protocol address, or routing code.</p> <p>Detection or discovery of a “Red Flag” implicates the need to take action under this ITPP to help prevent, detect, and correct identity theft.</p> <p>III. Detecting “Red Flags” For Potential Identity Theft</p> <p>A. Risk Factors for Identifying “Red Flags” The College will consider the following factors in identifying relevant “Red Flags:”</p> <ol style="list-style-type: none"> 1) the types of covered accounts the College offers or maintains; 2) the methods the College provides to open the College's covered accounts; 3) the methods the College provides to access the College's covered accounts; and 4) the College's previous experience(s) with identity theft. <p>B. Sources of “Red Flags” The College will continue to incorporate relevant “Red Flags” into this ITPP from the following sources:</p>
---	---	--

<p>Red Flags</p> <ol style="list-style-type: none"> 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 information; and 4. Application for service that appears to have been altered or forged. <p>C. Suspicious Personal Identifying Information</p> <p>Red Flags</p> <ol style="list-style-type: none"> 1. Identifying information presented that is inconsistent with other information the person provides (example: inconsistent birth dates); 2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application); 3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent; 	<ol style="list-style-type: none"> 3) guidance from the [entity's supervisor's who identify changes in identity theft risks. <p>C. Categories of "Red Flags"</p> <p>The following Red Flags have been identified for the [entity]'s covered accounts:</p> <p>Alerts, Notifications, or Warnings from a Consumer Reporting Agency:</p> <ol style="list-style-type: none"> 1) A fraud or active duty alert is included with a consumer report the [entity] receives as part of a background check. 2) A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report. 3) A consumer reporting agency provides a notice of address discrepancy. An address discrepancy occurs when an address provided by a student substantially differs from the one the credit reporting agency has on file. See Section (V)(9) for specific steps that must be taken to address this situation. 	<ol style="list-style-type: none"> 1) incidents of identity theft that the College has experienced; 2) methods of identity theft that the College identifies that reflects changes in identity theft risks; and 3) guidance from the College's staff who identify changes in identity theft risks. <p>C. Categories of "Red Flags"</p> <p>The following Red Flags have been identified for the College's covered accounts:</p> <p>Alerts, Notifications, or Warnings from a Consumer Reporting Agency:</p> <ol style="list-style-type: none"> 1) A fraud or active duty alert is included with a consumer report the College receives as part of a background check. 2) A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report. 3) A consumer reporting agency provides a notice of address discrepancy. An address discrepancy occurs when an address provided by a student or an employee substantially differs from the one the credit reporting agency has on file. See Section (V)(10) for specific
--	--	---

<p>4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);</p> <p>5. Social security number presented that is the same as one given by another person;</p> <p>6. An address or phone number presented that is the same as that of another person;</p> <p>7. A person fails to provide complete personal identifying information on an application when reminded to do so; and</p> <p>8. A person's identifying information is not consistent with the information that is on file.</p> <p>D. Suspicious Covered Account Activity or Unusual Use of Account Red Flags</p> <p>1. Change of address for an account followed by a request to change the account holder's name;</p> <p>2. Payments stop on an otherwise consistently up-to-date account;</p> <p>3. Account used in a way that is not consistent with prior use;</p> <p>4. Mail sent by the College is repeatedly returned as undeliverable;</p>	<p>4) A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant, such as:</p> <ul style="list-style-type: none"> (a) A recent and significant increase in the volume of inquiries; (b) An unusual number of recently established credit relationships; (c) A material change in the use of credit, especially with respect to recently established credit relationships; or (d) An account that was closed for cause or identified for abuse of account privileges by a creditor or financial institution. <p>Suspicious Documents:</p> <ul style="list-style-type: none"> 1) Documents provided for identification appear to have been forged or altered. 2) The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification. 	<p>steps that must be taken to address this situation.</p> <p>4) A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant, such as:</p> <ul style="list-style-type: none"> (a) A recent and significant increase in the volume of inquiries; (b) An unusual number of recently established credit relationships; (c) A material change in the use of credit, especially with respect to recently established credit relationships; or (d) An account that was closed for cause or identified for abuse of account privileges by a creditor or financial institution. <p>Suspicious Documents:</p> <ul style="list-style-type: none"> 1) Documents provided for identification appear to have been forged or altered. 2) The photograph or physical description on the identification is not consistent with the appearance of the applicant or
---	---	--

5. Notice to the College that a person is not receiving mail sent by the College;

6. Notice to the College that an account has unauthorized activity;

7. Breach in the College's computer system security; and

8. Unauthorized access to or use of account information.

E. Alerts from Others
Red Flag

1. Notice to the College from a student, Identity Theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

IV. DETECTING RED FLAGS
A. Student Enrollment / New Employee and Other Persons Accounts

In order to detect any of the Red Flags identified above associated with the enrollment of a student, new employees or other persons, College 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

3) Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

4) Other information on the identification is not consistent with readily accessible information that is on file with the [**entity**], such as a signature card or a recent check.

5) An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

Suspicious Personally Identifying Information:

1) Personal identifying information provided is inconsistent when compared against external information sources used by the [**entity**]:

For example:

(a) The address does not match any address in the consumer report; or

(b) The Social Security Number (SSN) has

customer presenting the identification.

3) Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

4) Other information on the identification is not consistent with readily accessible information that is on file with the College, such as a signature card or a recent check.

5) An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

Suspicious Personally Identifying Information:

1) Personal identifying information provided is inconsistent when compared against external information sources used by the College.

For example:

(a) The address does not match any address in the consumer report; or

<p>birth, academic records, home address or other identification; and</p> <p>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).</p> <p>B. Existing Accounts In order to detect any of the Red Flags identified above for an existing Covered Account, UCC personnel will take the following steps to monitor transactions on an account:</p> <p>Detect</p> <p>1. Verify the identification of persons if they request information (in person, via telephone, via facsimile, via email);</p> <p>2. Verify the validity of requests to change billing addresses by mail or email and provide reasonable means of promptly reporting incorrect billing address changes; and</p> <p>3. Verify changes in banking information given for billing and payment purposes.</p> <p>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 or background report is sought, College personnel will take the following steps</p>	<p>not been issued, or is listed on the Social Security Administration's Death Master File.</p> <p>2) Personal identifying information provided by a person is not consistent with other personal identifying information provided by the person. For example, there is a lack of correlation between the SSN range and date of birth.</p> <p>3) Personal identifying information is associated with known fraudulent activity as indicated by internal or third-party sources use by the [entity]. For example:</p> <p>(a) The address on an application is the same as the address provided on a fraudulent application;</p> <p>(b) The phone number on an application is the same as the phone number provided on a fraudulent application;</p> <p>4) Personal identifying information provided is of a type commonly associated with</p>	<p>(b) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.</p> <p>2) Personal identifying information provided by a person is not consistent with other personal identifying information provided by the person. For example, there is a lack of correlation between the SSN range and date of birth.</p> <p>3) Personal identifying information is associated with known fraudulent activity as indicated by internal or third-party sources use by the College. For example:</p> <p>(a) The address on an application is the same as the address provided on a fraudulent application;</p> <p>(b) The phone number on an application is the same as the phone number provided on a fraudulent application;</p>
--	---	--

<p>to assist in identifying address discrepancies:</p> <p>1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the background check or credit report is made to the consumer reporting agency; and</p> <p>2. In the event that notice of an address discrepancy is received, verify that the background check or 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 College has reasonably confirmed is accurate.</p> <p>V. PREVENTING AND MITIGATING IDENTITY THEFT</p> <p>In the event Umpqua Community College personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:</p> <p>Prevent and Mitigate</p> <p>1. Continue to monitor a Covered Account for evidence of Identity Theft;</p> <p>2. Contact the student or applicant (for which a background check or credit report was run);</p>	<p>fraudulent activity as indicated by internal or third-party sources used by the [entity]. For example:</p> <p>(a) The address on an application is fictitious, a mail drop, or a prison; or</p> <p>(b) The phone number is invalid, or is associated with a pager or answering service.</p> <p>5) The SSN provided is the same as that submitted by other persons currently being served by the [entity].</p> <p>6) The address or telephone number provided is the same or similar to the account number or telephone number submitted by an unusually large number of other persons being served by the [entity].</p> <p>7) The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.</p> <p>8) Personal identifying information provided is not</p>	<p>4) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the College. For example:</p> <p>(a) The address on an application is fictitious, a mail drop, or a prison; or</p> <p>(b) The phone number is invalid, or is associated with a pager or answering service.</p> <p>5) The SSN provided is the same as that submitted by other persons currently being served by the College.</p> <p>6) The address or telephone number provided is the same or similar to the account number or telephone number submitted by an unusually large number of other persons being served by the College.</p> <p>7) The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.</p>
---	--	---

<p>3. Change any passwords or other security devices that permit access to Covered Accounts;</p> <p>4. Not open a new Covered Account;</p> <p>5. Provide the person with a new identification number;</p> <p>6. Notify the Program Administrator for determination of the appropriate step(s) to take;</p> <p>7. Notify law enforcement;</p> <p>8. File or assist in filing a Suspicious Activities Report (“SAR”); or</p> <p>9. Determine that no response is warranted under the particular circumstances.</p> <p>Protect Identifying Information In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect identifying information:</p> <p>1. Ensure that its website is secure or provide clear notice that the website is not secure;</p> <p>2. Ensure complete and secure destruction of paper documents and computer files containing account information when a decision has been</p>	<p>consistent with personal identifying information that is on file with the [entity].</p> <p>9) The person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.</p> <p>Unusual Use Of – Or Suspicious Activity Relating To – A Covered Account:</p> <p>1) A new covered account is used in a manner that is commonly associated with known patterns of fraud patterns. For example, a person makes a first payment, but there are no subsequent payments made.</p> <p>2) A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example, there is:</p> <p>(a) Nonpayment when there is no history of late or missed payments; or</p> <p>(b) A material change in electronic fund transfer patterns in</p>	<p>8) Personal identifying information provided is not consistent with personal identifying information that is on file with the College.</p> <p>9) The person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.</p> <p>Unusual Use Of – Or Suspicious Activity Relating To – A Covered Account:</p> <p>1) A new covered account is used in a manner that is commonly associated with known patterns of fraud patterns. For example, a person makes a first payment, but there are no subsequent payments made.</p> <p>2) A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example, there is:</p> <p>(a) Nonpayment when there is no history of late or missed payments; or</p> <p>(b) A material change in electronic fund transfer patterns in</p>
--	---	--

<p>made to no longer maintain such information;</p> <p>3. Ensure that office computers with access to Covered Account information are password protected;</p> <p>4. Avoid use of social security numbers;</p> <p>5. Ensure computer virus protection is up to date; and</p> <p>6. Require and keep only the kinds of information that are necessary for College purposes.</p> <p>VI. PROGRAM ADMINISTRATION A. Oversight Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee (“Committee”) for the College. The Committee is headed by a Program Administrator who may be the President of the College or his or her appointee. Two or more other individuals appointed by the President of the College or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for ensuring appropriate training of College staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and</p>	<p>connection with a payment.</p> <p>3) A covered account that has been inactive for a reasonably lengthy period of time is suddenly used or active.</p> <p>4) Mail sent to the person holding the covered account is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the person’s covered account.</p> <p>5) The [entity] is notified that the person is not receiving paper account statements.</p> <p>6) The [entity] is notified of unauthorized transactions in connection with a person’s covered account.</p> <p>Notices From Customers/Persons, Victims of Identity Theft, Law Enforcement Authorities, or Other Businesses About Possible Identity Theft in Connection with Covered Accounts:</p> <p>The [entity] is notified by a person with a covered account, a victim of identity theft, a law enforcement</p>	<p>connection with a payment.</p> <p>3) A covered account that has been inactive for a reasonably lengthy period of time is suddenly used or active.</p> <p>4) Mail sent to the person holding the covered account is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the person’s covered account.</p> <p>5) The College is notified that the person is not receiving paper account statements.</p> <p>6) The College is notified of unauthorized transactions in connection with a person’s covered account.</p> <p>Notices From Customers/Persons, Victims of Identity Theft, Law Enforcement Authorities, or Other Businesses About Possible Identity Theft in Connection with Covered Accounts:</p> <p>The College is notified by a person with a covered account, a victim of identity theft, a law enforcement</p>
---	--	---

<p>mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.</p> <p>B. Staff Training and Reports</p> <p>College 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. College staff shall be trained, as necessary, to effectively implement the Program. College employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the College's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, College 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,</p>	<p>authority, or any other person, that it has opened a fraudulent account for a person engaged in identity theft.</p> <p>IV. Measures to Detect "Red Flags"</p> <p>The [entity] shall do the following to aid in the detection of "Red Flags:"</p> <p>1) When a new covered account is open, the [entity] shall obtain identifying information about, and information verifying the identity of, the student or other person seeking to open a covered account. Two forms of identification shall be obtained (at least one of which must be a photo identification).</p> <p>The following are examples of the types of valid identification that a person may provide to verify the identity of the person seeking to open the covered account: valid state-issued driver's license, valid state-issued identification card, current passport, a Social Security Card, current residential lease, or copy of a deed to the person's home or</p>	<p>authority, or any other person, that it has opened a fraudulent account for a person engaged in identity theft.</p> <p>IV. Measures to Detect "Red Flags"</p> <p>The College shall do the following to aid in the detection of "Red Flags:"</p> <p>1) When a new covered account is open, the College shall obtain identifying information about, and information verifying the identity of, the student or other person seeking to open a covered account. Two forms of identification shall be obtained (at least one of which must be a photo identification).</p> <p>The following are examples of the types of valid identification that a person may provide to verify the identity of the person seeking to open the covered account: valid state-issued driver's license, valid state-issued identification card, current passport, a Social Security Card, current residential lease, or copy of a deed to the person's home or</p>
--	--	--

<p>and recommendations for changes to the Program.</p> <p>C. Service Provider Arrangements In the event the College engages a service provider to perform an activity in connection with one or more Covered Accounts, the College 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.</p> <ol style="list-style-type: none"> 1. Require, by contract, that service providers have such policies and procedures in place; and 2. Require, by contract, that service providers review the College's Program and report any Red Flags to the Program Administrator or the College employee with primary oversight of the service provider relationship. <p>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 who developed this Program 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</p>	<p>invoice/statement for property taxes.</p> <p>2) Persons with covered accounts who request a change in their personal information on file, such as a change of address, will have the requested changes verified by the [entity].</p> <p>The person shall provide at least one written form of verification reflecting the requested changes to the personal information. For example, if an address change is requested, then documentation evidencing the new address shall be obtained. If a phone number change is requested, then documentation evidencing the new phone number, such as a phone bill, shall be obtained.</p> <p>V. Preventing and Mitigating Identity Theft One or more of the following measures, as deemed appropriate under the particular circumstances, shall be implemented to respond to "Red Flags" that are detected:</p> <ol style="list-style-type: none"> 1) Monitor the covered account for evidence of identity theft; 	<p>invoice/statement for property taxes.</p> <p>2) Persons with covered accounts who request a change in their personal information on file, such as a change of address, will have the requested changes verified by the College.</p> <p>The person shall provide at least one written form of verification reflecting the requested changes to the personal information. For example, if an address change is requested, then documentation evidencing the new address shall be obtained. If a phone number change is requested, then documentation evidencing the new phone number, such as a phone bill, shall be obtained.</p> <p>V. Preventing and Mitigating Identity Theft One or more of the following measures, as deemed appropriate under the particular circumstances, shall be implemented to respond to "Red Flags" that are detected:</p>
---	--	---

<p>describe such specific practices and the information those documents contain are considered “confidential” and should not be shared with other employees or the public. The Program Administrator shall inform the Committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.</p> <p>E. Program Updates</p> <p>The Committee will periodically review and update this Program to reflect changes in risks to students, employees / other persons and the soundness of the College from Identity Theft. In doing so, the Committee will consider the College's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the College's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.</p>	<ol style="list-style-type: none"> 2) Contact the person who holds the covered account; 3) Change any passwords, security codes, or other security devices that permit access to a covered account; 4) Reopen the covered account with a new account number; 5) Not open a new covered account for the person; 6) Close an existing covered account; 7) Not attempt to collect on a covered account or not sell a covered account to a debt collector; 8) Notifying law enforcement; 9) Where a consumer reporting agency provides an address for a consumer that substantially differs from the address that the consumer provided, the [entity] shall take the necessary steps to for a reasonable belief that the [entity] knows the identity of the person for whom the [entity] obtained a credit report, and reconcile the address of the consumer with the credit reporting agency, if the [entity] establishes a continuing relationship with the consumer, and regularly, and in the course of 	<ol style="list-style-type: none"> 1) Monitor the covered account for evidence of identity theft; 2) Contact the person who holds the covered account; 3) Change any passwords, security codes, or other security devices that permit access to a covered account; 4) Reopen the covered account with a new account number; 5) Not open a new covered account for the person; 6) Close an existing covered account; 7) Notify the Program Administrator for determination of the appropriate step(s) to take; 8) Not attempt to collect on a covered account or not sell a covered account to a debt collector; 9) Notifying law enforcement; 10) Where a consumer reporting agency provides an address for a consumer that substantially differs from the address that the consumer provided, the College shall take the necessary steps to for a reasonable belief that the College knows the identity of the person for whom the College obtained a credit
--	--	---

	<p>business, provides information to the credit reporting agency; or</p> <p>10) Determine that no response is warranted under the particular circumstances.</p> <p>VI. Updating the ITPP The [<i>entity</i>] shall update this ITPP on an annual basis to reflect changes in risks to persons with covered accounts, or to reflect changes in risks to the safety and soundness of the [<i>entity</i>] from identity theft, based on the following factors:</p> <ol style="list-style-type: none"> 1) The experiences of the [<i>entity</i>] with identity theft; 2) Changes in methods of identity theft; 3) Changes in methods to detect, prevent and mitigate identity theft; 4) Changes in the types of covered accounts that the [<i>entity</i>] maintains; 5) Changes in the business arrangements of the [<i>entity</i>], including service provider arrangements. <p>VII. Methods for Administering the ITPP</p> <p>A. Oversight of the ITPP Oversight by the 's [<i>designate position</i>] shall include:</p>	<p>report, and reconcile the address of the consumer with the credit reporting agency, if the College establishes a continuing relationship with the consumer, and regularly, and in the course of business, provides information to the credit reporting agency; or</p> <p>11) Determine that no response is warranted under the particular circumstances.</p> <p>VI. Protect Identifying Information In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect identifying information:</p> <ol style="list-style-type: none"> 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 account 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;
--	---	---

	<ol style="list-style-type: none"> 1) Assigning specific responsibility for the ITPP's implementation; 2) Reviewing reports prepared by the staff regarding compliance of the ITPP; and 3) Approving material changes to the ITPP as necessary to address changing identity theft risks. <p>B. Reports</p> <ol style="list-style-type: none"> 1) In General – Staff responsible for the development, implementation, and administration of this ITPP shall report to the Board of Education on an annual basis. 2) Contents of Report – The report shall address material matters to the ITPP and evaluate the following issues: the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with opening new covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's 	<ol style="list-style-type: none"> 4. Avoid use of social security numbers; 5. Ensure computer virus protection is up to date; and 6. Require and keep only the kinds of information that are necessary for College purposes. <p>VII. Updating the ITPP The College shall update this ITPP on an annual basis to reflect changes in risks to persons with covered accounts, or to reflect changes in risks to the safety and soundness of the College from identity theft, based on the following factors:</p> <ol style="list-style-type: none"> 1) The experiences of the College with identity theft; 2) Changes in methods of identity theft; 3) Changes in methods to detect, prevent and mitigate identity theft; 4) Changes in the types of covered accounts that the College maintains; 5) Changes in the business arrangements of the College, including service provider arrangements. <p>VIII. Methods for Administering the ITPP Oversight of the ITPP</p>
--	--	---

	<p>response; and recommendations for material changes to the ITPP.</p> <p>3) Oversight of Service Provider Arrangements – Whenever the [entity] engages a service provider to perform an activity in connection with one or more covered accounts the [entity] shall take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. To that end, the [entity] shall require our service contractors, by contract, to have policies and procedures to detect relevant “Red Flags” that may arise in the performance of the service provider’s activities, and either report the “Red Flags” to the [entity], or to take appropriate steps to prevent or mitigate identity theft.</p>	<p>Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee (“Committee”) ^[INB1] for the College. The Committee is headed by a Program Administrator who may be the President of the College or his or her appointee. Two or more other individuals appointed by the President of the College or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for ensuring appropriate training of College 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.</p> <p>Oversight by the Program Administrator shall include:</p> <ol style="list-style-type: none"> 1) Assigning specific responsibility for the ITPP’s implementation; 2) Reviewing reports prepared by the staff regarding compliance of the ITPP; and 3) Approving material changes to the ITPP as necessary to
--	---	--

		<p>address changing identity theft risks.</p> <p>D. Reports</p> <p>1) In General – Staff responsible for the development, implementation, and administration of this ITPP shall report to the Program Administrator on an annual basis.</p> <p>2) Contents of Report – The report shall address material matters to the ITPP and evaluate the following issues: the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with opening new covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management’s response; and recommendations for material changes to the ITPP.</p> <p>3) Oversight of Service Provider Arrangements – Whenever the College engages a service provider to perform an activity in connection with one or more covered accounts the College shall take steps to ensure that</p>
--	--	---

		<p>the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. To that end, the College shall require our service contractors, by contract, to have policies and procedures to detect relevant “Red Flags” that may arise in the performance of the service provider’s activities, and either report the “Red Flags” to the College, or to take appropriate steps to prevent or mitigate identity theft.</p> <p>Reference: 15 U.S. Code Section 1681m(e) (Fair and Accurate Credit Transactions Act (FACT ACT or FACTA))</p> <p>ORS 646A.604(8) (notice exception – Oregon Consumer Identity Theft Protection Act)</p> <p>RESPONSIBILITY: The CFO is responsible for implementing and updating this procedure.</p>
--	--	--

<p>BOARD OF EDUCATION UMPQUA COMMUNITY COLLEGE DOUGLAS COUNTY, OREGON</p>	<p><input type="checkbox"/> Information Item <input checked="" type="checkbox"/> Action Item</p>
<p>Subject: Personnel Employment Agreements</p>	<p>Date: April 08, 2020</p>
<p>Board approval is requested to award contracts for Administrator/Confidential Exempt employees and contracts for probationary and regular Faculty for the 2020-2021 fiscal year.</p>	
<p>Recommendation by:</p> 	<p>Approved for Consideration:</p> 

**Salary Recommendations - Full-Time Faculty
Fiscal Year 2020-2021**

Renew Regular Faculty Status:

Alan Aylor	Kevin Mathweg
R. Clay Baumgartner	Michael Matteo
Melinda Benton	Shauna McNulty
John Blackwood	Jillanne Michell
John Blakely	April Myler
Sean Breslin	Tafea Polamalu
Toni Clough	Joanne Richards
Patrice Coate	Susan Rochester
L. Mick Davis	Emery Smith
Amy Fair	Gregg Smith
Ian Fisher	Rod Snook
Marie Gambill	Cynthia Steele
Gary Gray	Mary Stinnett
Patrick Harris	David Stricklin
Jason Heald	Crystal Sullivan
Andre' Jacob	Duane Thompson
Martha Joyce-Test	Nicholas Tratz
Roger Kennedy	Joseph Villa
Stuart Kramer	Georgann Willis
Jennifer Lantrip	R. Dee Winn
Daniel Leeworthy	David Wolf
Brent Lewis	Vincent Yip
Tamara Loosli	Charles Young

Award Regular Faculty Status:

Doyle Poole
Lesa Beth Titus

Renew Probationary Contract Status:

Christina Allaback	Alexander Jardon
Bryan Benz	Alan King
Peter Chamberlain	Sheryl Lehi
Hanna Culbertson	Jeremiah Robbins
Jan Dawson	Leslie Rogers
Alyssa Harter	Jarred Saralecos

Renew Regular Faculty Status - Soft Money/Grants, Contracts & Other:

(Contingent upon funding from outside sources)

Renew Probationary Contract Status - Soft Money/Grants, Contracts & Other:

(Contingent upon funding from outside sources)

Nathan Anderson
Sean Mock

**Contract Renewals
Administrators and Confidential/Exempt Staff
Fiscal Year 2020-2021**

Administrators/Confidential-Exempt - Award One-Year Contract:

Michelle Bergmann	Jess Miller
Natalya Brown	Jason "Mitch" Mitchell
Tiffany Coleman	Missy Olson
Sue Cooper	Jessica Richardson
Kacy Crabtree	Steven Rogers
Jules DeGiulio	Micque Shoemaker
Rosario Fauver	Andrew Swan
April Hamlin	Robin VanWinkle
Brenna Hobbs	Robynne Wilgus
Craig Jackson	Katie Workman
Carol McGeehon	

Administrators/Confidential-Exempt - Continuation of Probationary Contract:

Daniella Bivens (9/4/19-9/3/20)	Whitney Pitalo (11/18/19-11/17/20)
Danielle Haskett (9/12/19-9/11/20)	Kelley Plueard (2/19/20-2/18/21)
Tim Hill (9/1/19-8/31/20)	Robin Van Winkle (03/30/2020-03/29/2021)
Ina Jackson	Kristen Watson (11/14/19-11/13/20)
Kimberly Meinhardt (4/6/20-4/5/21)	Lisa Woods (1/21/20-1/20/21)

**Administrator/Confidential-Exempt - Award One-Year Contract
Funding Sources Other Than General Funds:**

Marjan Coester

**Administrator/Confidential-Exempt - Award One-Year Contract
Contingent Upon Funding From Outside Sources:**

Ellen Brown	Heather Freiling
Melinda Collier	Mary Morris

**Administrator/Confidential-Exempt - Continuation of Probationary Contract
Contingent Upon Funding From Outside Sources:**

--