ACADEMIC AFFAIRS

FORM 1: Presentation Checklist

Please review the following list of items that must be considered by new programs or significant changes to current programs or policy. Not every item listed is required for each presentation to Academic Affairs. This list serves as a review of potential questions addressed by the Academic Affairs Committee.

Facilitators of new or changing programs or policy should work closely with the curriculum coordinator, appropriate department chair(s) and instructional dean, or with appropriate administrative leadership to review the following list, prior to the first reading with Academic Affairs.

Please note: If an item listed is not relevant to your specific presentation to Academic Affairs, please mark it as **N/A**. Use the last page for your remarks.

OVERVIEW OF PROGRAM OR POLICY

□ Give rational for new program or changes in current program or policy, including data to support rationale (attach any necessary documents).

BUDGET

□ Review key budget items.

- Revenue projections based on student enrollment projections or other sources of income, including tuition and fees.
- Start-up budget requirements including salary, benefits, materials and supplies, equipment, facilities
- Post implementation budget including salary, benefits, materials and supplies, equipment, facilities, etc.

INSTRUCTIONAL REQUIREMENTS

□ Review requirements.

- Current availability of faculty, administration and/or staff.
- Minimum qualifications for faculty, administration and/or staff.
- Potential impacts to all affected academic and other departments.

OPERATIONAL NEEDS, CURRENT AND FUTURE

□ Review possible operational needs.

- Existing resources including faculty, administration, staff, equipment.
- Involvement of department with oversight of program or process
- Required administrative support.
- Facility needs, including location, amount of space, construction or remodeling requirements.
- Potential impacts to administrative and student support departments including Enrollment services, Financial Aid, CAP Center, Library, Tutoring and Testing, Information Technology Services and others.

STUDENT IMPACT

□ Identify student impact

- Identify and quantify potential student impact.
- Minimize negative student impact through teach-outs, grandfather clauses, substitutions or other options.
- Communication planning.

ANTICIPATED IMPLEMENTATION TIMELINE

□ Anticipated Timeline

- Designate affected department(s) and include names and positions of faculty, administration and staff involved in implementation.
- Identify current process adjustments.
- Change General Procedures Manual as needed.
- Communication planning.

Academic Affairs Presentation Checklist

Name: Ralph Phillips **Date**: 11/14/2017

Department: Computer and Information Systems (CIS)

Please note: If an item listed is not relevant to your specific presentation to Academic Affairs, please mark as **N/A**. Use as many pages as necessary.

OVERVIEW OF PROGRAM OR POLICY

Short-term Certificate in Cybersecurity

The CIS Cybersecurity short-term certificate is a 4-class (14-credit) suite of courses designed to prepare CIS Networking, Computer Science students and/or existing industry professionals to qualify for entry-level jobs categorized as either Junior Information Security Analysts or Cybersecurity technicians.

Course	Course Title	Credits	Industry Certification
CIS 101 (NEW)	**Cyber Program Orientation *****	**2**	**N/A**
CIS 279SE	Security+	4	CompTIA Security+
CIS 284EH	Ethical Hacking	4	EC-Council Certified Ethical Hacking
CIS 284	CCNA Security	4	Cisco Security

BUDGET

- This would be a 14-credit certificate, with no additional costs for creation and startup.
- Students would will be encouraged to pass 3 industry certifications along the way or soon after completion. These certifications tests range in cost from $100 - $200.

INSTRUCTIONAL REQUIREMENTS

- Existing faculty in the CIS department can teach all of the classes. Most classes in this program are already offered in CIS as part of existing AAS degrees. One new 2-credit class would be created.
- Possible that we will seek out a replacement FT faculty with cybersecurity/networking skills when needing to replace retiring FT faculty in the next 2-3 years.
- New instructional hires would need computer networking experience and cybersecurity experience. Instructors may have a Bachelor's degree with appropriate experience.
- It is not likely that other COCC departments will be affected. It is likely that most students completing the certificate are working on a larger AAS. Other students may be working professionals looking to add cybersecurity skills to their networking training/experience.

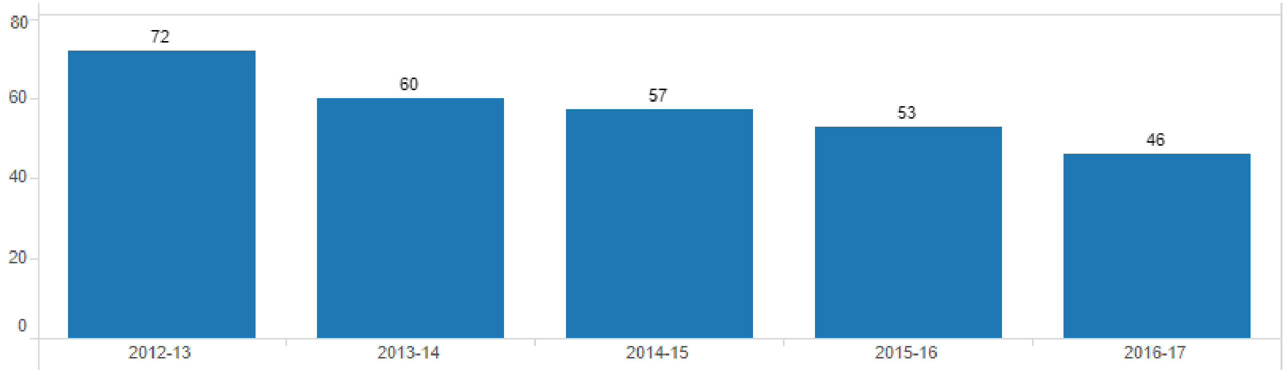
OPERATIONAL NEEDS, CURRENT AND FUTURE

- We expect to utilize existing staff and resources, including a networking lab/classroom in Pioneer Hall 232.
- We do NOT expect any additional impacts on administrative and student support departments.

STUDENT IMPACT

- Marketing and education of the program will be critical. The department will work to promote the program to students and solicit help from COCC public relations.
- There is potential that this short-term cert will be valuable to local computer networking professionals. We will seek out ways to advertise this program to non-degree seeking students.
- A partnership with community education may be established for these courses.
- Students in entry-level networking classes will get informed about the cybersecurity certificate.
- CIS Advisors will also make sure students know about the option of a short-term certificate while working towards another academic goal.

Networking Students



- Students seeking the certificate may be 10-15 during the first year.
- Networking students will be the likely “early adopters” of the Cybersecurity certificate. Many will have taken some of the certificate classes already and need to finish one more and the 2-credit orientation course.
- We expect enrollment to increase each year after, based on existing programs at other schools, advice from advisory partners (cybersecurity employers in Bend), and growing opportunities in the job market.

ANTICIPATED IMPLEMENTATION TIMELINE

- We would like this certificate listed in the catalog for AY 18-19.
- Students that start the cert, will likely be existing CIS Networking students.
- One new 2-credit orientation course will be available in 18-19.
- Advertisements to the public can take place during 18-19, for new students in 19-20.

- Students may complete this cert over a 2- or 3-term period. When enrollment and popularity increase, we may be able to offer the certification courses over a 1- or 2-term period.

New CTE Program Development Process
Stage 1: Program Abstract Proposal

The "Program Abstract" is the first step for those individuals or teams interested in proposing a new career and technical education (CTE) program. When complete, submit the information to the Vice President for Instruction, who will solicit feedback from the President's Advisory Team and the President. The president may then approve the abstract as is, ask for additional information, or deny the proposal.

Details regarding the full process for developing new CTE programs is available through the Vice President for Instruction's office.

Proposer(s): **CIS Department (Dan Alberghetti, Eric Magidson, Ralph Phillips)**

1. **Program Overview:** Provide a general description of the program and program goals. If the program needs to start quickly, the proposer should indicate whether the program should be offered in a non-credit format and a plan to transition it to credit offerings. If program courses were previously offered as noncredit courses, describe program enrollment trends, program history, and other lessons learned from the noncredit offerings.

   The CIS Cybersecurity short-term certificate is a 4-class (14-credit) suite of courses designed to prepare CIS Networking, Computer Science students and/or existing industry professionals to qualify for entry-level jobs categorized as either Information Security Analysts or Cybersecurity technicians.

   Proposed Classes:

Course	Course Title	Credits	New or Existing	Industry Certification
CIS***	Into to Cybersecurity	2	New	N/A
CIS279SE	Security +	4	Existing	CompTia Security+ -SY0-401
CIS284EH	Ethical Hacking	4	Existing	EC-Council Certified Ethical Hacking (312-50 VUE)
CIS284	CCNA Security	4	Existing	Cisco Security (210-260 IINS)
There is a proposal being considered to remove these courses from the CIS Networking Option and create a more focused prefix (CYB = Cyber) to better create guided pathways and meet national program (National Security Administration) requirements.				

2. **Strategic Alignment:** Describe how the new program fits with the COCC mission, strategic plan, and accreditation core themes.

   As related to the Core Themes, the new Cybersecurity program would support:

1. Workforce Development
WD 2. Deliver CTE curricula that meets current industry standards.
WD.3 Maintain and strengthen student opportunities in CTE programs for students to achieve program completion and employment in their area of study.

2. Lifelong Learning
LL.1 Broaden lifelong learning opportunities based on assessed industry, community, and campus needs.
LL.3 Expand options for accessibility and instructional delivery in Continuing Education.

As Related to Strategic Plan, the new Cybersecurity program would support:

1. **Our Vision**
   ***Preparing "students for employment"**
   ***Assisting "regional employers"**

3. **Employment Projections:** Provide evidence of employment opportunities after program completion, including anticipated wage upon entry, wage progression potential and a statement of need for the occupation. Possible resources include: Oregon Labor Market Information System (OLMIS); discussion with the regional economist (541.388.6442 or 541.306.1645); and the U.S. Bureau of Labor Statistics. Professional organizations and other data sources may also be used.

   The labor market analysis should include regional and national data on the following questions, noting that both Central Oregon and national trends may be considered:

   a. Why is this program necessary? **It will help to educate students into the fastest growing (demanded) area within Computer Information Systems (CIS).**
   b. Does the workforce data show that the proposed program is needed? **Yes.**
   c. Can training be provided without creating a new program? **A degree, see additional proposal, and this certificate will provide focused completers in this area of CIS.**
   d. What other data resources have been utilized in addition to the Employment Department, e.g., professional organizations, national census, and regional workforce specialists? **Conference calls with local industry professionals, graduation rates from MHCC, see below, and articles citing the growing demand.**
   e. What career pathways, employment opportunities, and further educational opportunities exist for students who complete the program? **We will be working with Oregon Institute of Technology to create a transfer agreement for 12 of the certificate courses to transfer into their Bachelors of Information Technology degree they will begin to offer Fall of 2018. *This degree may be completed all online.**

1. **Oregon Occupation & Wage Information shows the lowest 10% of starting jobs as paying $24-$35 per hour ($49,920 to $72.800 per year). For Oregon, this job is expected to grow at a "somewhat faster rate than the statewide average growth rate**

for all occupations through 2024.” (Reference Link)

2. **Bureau of Labor Statistics, Information Security Analyst median pay is $45 per hour ($93,600 per year). Jobs are expected to “grow much faster than average” at 18% for 2014-2024. (Reference Link)**

3. **CSO Online (June 2017): Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021. In 2017, the U.S. employs nearly 780,000 people in cybersecurity positions, with approximately 350,000 current cybersecurity openings, according to CyberSeek, a project supported by the National Initiative for Cybersecurity Education (NICE), a program of the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce. (Reference Link)**

4. **Mount Hood Community College: Data provided by Wayne Machuca, ISTM/CyberSecurity Program Director.**

5.	2011-2012	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017
CIS Grads	34	44	49	82	67	69
ISTM/Cyber				42	66	104

We just Compiled these for a grant we are doing” – Wayne Machuca
****CIS will include Game, the legacy degrees: Networking and OS, web master, and IT tech.**
****ISTM will include CyberSecurity and Networking and CS/Database.**

5. **Federal IT Security Leaders Push for More Training to Boost Cybersecurity Response. The Trump administration’s executive order on cybersecurity gives agencies enough direction to guide investments in education and training, officials say. (Reference Link)**

*Jobs in Information Security / Cybersecurity are not location specific and thus graduates of our program could “telecommute” and thus work for companies all around the world while continuing to live in and contribute to the Central Oregon community.

4. **Implementation Timeline:** The typical timeline for implementing a new CTE program is included in Appendix A. Describe the anticipated timeline for program implementation, indicating any modifications to the traditional timeline described in Appendix A. Note that the timeline provided is for a traditional start up only; *extraordinary* resources may allow a more rapid implementation timeline and should be explained in the program proposal.

First course(s) of the series would be available in Fall 2018, with remaining courses offered in Winter and Spring of 2019.

5. **Organizational Structure and Implementation Team:** Identify campus faculty and staff who will be involved in implementing this program, including the program developer, the department to which this program will report, and the chair, dean and other implementation team members. Include specific names and at what stage it is anticipated that a content expert may need to be hired.

Lead Faculty: Eric Magidson (Program Developer) and Dan Alberghetti

Department:	**Computer and Information Systems (CIS)**
Chair:	**Ralph Phillips**
Dean:	**Michael Fisher**

6. **Specialized Accreditation:** Indicate whether the program requires specialized accreditation and any known accreditation requirements which may impact program delivery, staffing, budget, or other factors.

   Although special accreditation is not required, earning the National Security Administration (NSA)/ Department of Homeland Security (DHS) National Centers of Academic Excellence in Cyber Defense Two-Year Education (CAE-2Y) accreditation will provide nationally recognized and marketable support for our program. *Enrollment in the ISTM program at Mount Hood Community College doubled within one year of their accreditation.

   This accreditation will require a great deal of work, program and course specific changes, submitted and approved by the curriculum committee, over the next year to meet the knowledge unit mappings required in every course within the new certification and proposed AAS in Cybersecurity degree.

7. **Diversity:** Explain how this program may help support or foster diversity of our student population, academic programs, values, or other considerations.

   We have begun to work with the Central Oregon STEM coordinator, Whitney Swander, to review opportunities to better market/promote careers in CIS and Cybersecurity to the woman, Hispanics, and Tribal Members, who traditionally are identified as minority demographic groups within this area.

8. **Exceptional Needs:** Describe extraordinary needs anticipated as a result of this program; this includes teaching and/or support staff, facilities, policy changes, accreditation requirements or other considerations.

   Given the relative newness of cybersecurity, as a focus area within CIS, current COCC instructors will need to be greatly supported with continued educational opportunities that will provide the skills and potential industry certification training needed to successfully educate our students pursuing either the cyber security certificate or proposed degree.