

Docket Item:

Community College Approval: Mt. Hood Community College, Certificate of Completion in Business Cybersecurity Practical Implementation, within 11.1003, Computer and Information Systems Security.

Summary:

Mt. Hood Community College proposes a new Certificate of Completion in Business Cybersecurity Practical Implementation. Higher Education Coordinating Commission (HECC) staff completed a review of the proposed program. After analysis, HECC staff recommends approval of the degree as proposed.

Staff Recommendation:

The HECC recommends the adoption of the following resolution:

RESOLVED, that the Higher Education Coordinating Commission approve the following degree: CC in Business Cybersecurity Practical Implementation.



Mt. Hood Community College seeks the Oregon Higher Education Coordinating Commission's approval to offer an instructional program leading to a Certificate of Completion in Business Cybersecurity Practical Implementation.

Program Summary

The MHCC Cybersecurity Program is proposing adding a new Cybersecurity Certificate of Completion. The purpose of this credential is to present fundamental business cybersecurity skills and structures common to most small and medium sized businesses. This program is intended for individuals with basic computer awareness or have completed Credential I. In this program, students will be exposed to general cyber security topics in an up-to-date and investigatory environment, learn the language of computer hackers, learn general network design techniques, and create a business plan for the inevitable hack event.

1. *Describe the need for this program by providing clear evidence.*

There is a huge need to create small business cybersecurity certificates for the small business community. The Small Business Development Center, an extension of Mt Hood Community College, is required under the Small Business Administration to serve small businesses. Our team at the Mt Hood SBDC oversees the Oregon SBDC Statewide Cybersecurity Program. As part of our role, we work throughout the state to support awareness, education, advising and resources to small businesses on cybersecurity issues and concerns. Last year collectively the Oregon SBDC served more than 5,500 business and less than 1% have a strong cybersecurity infrastructure in place.

These businesses are not interested in going for a full two or four-year degree to obtain a job. They are business owners and are focused on receiving the most up-to-date cybersecurity knowledge so they can better support their business infrastructure. Many of them will never hire an IT team though the owners may take on the lead for creating a cybersecurity strategy plan.

Based on our work in the cybersecurity community we are fully aware of the following statistics:

- 43 percent of cyber attacks target small business;
- Only 14 percent of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective;
- 60 percent of small companies go out of business within six months of a cyber attack;
- 55 percent of respondents say their companies have experienced a cyber attack in the past 12 months (May 2015 -May 2016);
- 50 percent report they had data breaches involving customer and employee information in the past 12 months (May 2015 -May 2016);

- In the aftermath of these incidents, these companies spent an average of \$879,582 because of damage or theft of IT assets; and
- In addition, disruption to normal operations cost an average of \$955,429.

Small businesses reported that only:

- 38 percent regularly upgrade software solutions;
- 31 percent monitor business credit reports; and
- 22 percent encrypt databases.
- 75 percent of small businesses have no cyber risk insurance.

2. ***Does the community college utilize systemic methods for meaningful and ongoing involvement of the appropriate constituencies?***

This program has been created in collaboration with MHCC's office of instruction, the college wide curriculum committee, and the MHCC Small Business Development Center. Externally, the National Science Foundation through a grant received has requested this set of courses as part of building a program to support cybersecurity training particularly for small businesses in our community. We also rely on input from our cybersecurity advisory committee that consist of members from MHCC, Technology Association of Oregon, SBDC Michigan, and the National CyberSecurity Alliance. The advisory committee meets ten times a year to provide feedback and insight for our cybersecurity small business initiative.

3. ***Is the community college program aligned with appropriate education, workforce development, and economic development programs?***

The proposed Business Cybersecurity Fundamentals aligns with current Board goals of transforming lives and serving the community. In addition, it addresses the Partner Innovation core them where the college works closely with businesses to proactively reassess current and future trends so that it may provide relevant skills and educational training while eliminating barriers and maximizing efficiencies and service quality. Small Business owners completing the program will be more prepared in managing their cybersecurity strategies and engaging with up-to-date cybersecurity resources and tools. The curriculum was designed to provide small business owners with the knowledge and skills they need to meet the real concerns of cybersecurity threats. Special attention was taken to ensure that level of education and learning outcomes are clearly defined for this certificate as well as within each course. These outcomes align with the requirements for success in securing a small business and minimizing cybersecurity threats.

4. ***Does the community college program lead to student achievement of academic and technical knowledge, skills, and related proficiencies?***

This course of instruction includes training in HTML, Computer Concepts, Network +, Firewall, Digital Forensics, and Penetration Testing for defense.

5. ***Does the community college identify and have the resources to develop, implement, and sustain the program?***

The program will admit up to 30 students per Cybersecurity Cohort. Interested cybersecurity students may include recent potential entrepreneurs, solo entrepreneurs and small businesses referred from the Small Business Development Center, the Small Business Administration, Community Partners including the Technology Association of Oregon and employed business owners seeking to upgrade their skills and increase their knowledge and abilities.

Assurances

Mt. Hood Community College has met or will meet the four institutional assurances required for program application.

1. ***Access.*** The college and program will affirmatively provide access, accommodations, flexibility, and additional/supplemental services for special populations and protected classes of students.
2. ***Continuous Improvement.*** The college has assessment, evaluation, feedback, and continuous improvement processes or systems in place. For the proposed program, there will be opportunities for input from and concerning the instructor(s), students, employers, and other partners/stakeholders. Program need and labor market information will be periodically re-evaluated and changes will be requested as needed.
3. ***Adverse impact and detrimental duplication.*** The college will follow all current laws, rules, and procedures and has made good faith efforts to avoid or resolve adverse *intersegmental* and *intrasegmental* impact and detrimental duplication problems with other relevant programs or institutions.
4. ***Program records maintenance and congruence.*** The college acknowledges that the records concerning the program title, curriculum, CIP code, credit hours, etc. maintained by the Office are the official records and it is the college's responsibility to keep their records aligned with those of the Office. The college will not make changes to the program without informing and/or receiving approval from the Office.