Program Proposal Application

Complete the Program Proposal for new Associate of Applied Science degrees and Certificates of Completion. Include your Program Research/Evidence worksheet with this proposal when submitting to the Curriculum Committee. This information will be submitted to the state Higher Education Coordinating Committee for approval once the program goes through Lane's internal process. For help, contact the Curriculum Office.

Program Contact Information

Provide contact information (name, title, department, phone, e-mail)for the primary person responsible for coordinating the program.

Don Easton
Faculty Instructor
Computer Information Technology
eastond@lanecc.edu
Office: 541.463.5532; Cell: 541.214.1530

Program Details

Program Title	Cybersecurity
Awards Indicate type of award (Associate of Applied Science or AAS Option, Certificate of Completion)[1].	Associate of Applied Science
Classification of Instructional Programs (CIP)[2] family and number Example: 13) Education, 13.1001) Special Education and Teaching, General	11.1003) Computer and Information Systems Security/Information Assurance
Career Area (select one)	__Agriculture, Food, and Natural Resources Systems X_Arts, Information, and Communications __Business and Management __Health Services __Human Resources __Industrial and Engineering Systems

[1] If developing a certificate, is it related or independent? Related certificates are those in which the courses are wholly contained in a parent degree program. Certificates must be between 12-108 credits.

[2] Use this website to determine CIP code: https://nces.ed.gov/ipeds/cipcode/Default.aspx?y=55

Program Credits	92
Program Length	2 years
Proposed Start Date/Term	Fall 2019
Estimated Number of Students	40

Financial Assistance Options Available to Students in this Program (check or indicate all that apply)

Contact Financial Aid for help.

- ☑ Federal
- ☐ Workforce Innovation Opportunity Act
- ☑ State of Oregon
- ☑ Veterans Benefits
- ☑ College scholarships
- ☑ Private businesses, foundation aid: corp. reimbursement, scholarships
- ☐ Other (briefly describe):

Career Roadmap (required)

http://oregon.ctepathways.org/c/published/2318/lcc-cybersecurity.html

Program Advisory Committee members

List name, title, organization, contact information for each member. See Advisory Committees for more information about what the committees do. Advisory committees are required.

- Charles Laborn, Chief Technology Officer Partnered Solutions IT
- Ruby Porter Marketing + Design
- Scott Van Den Elzen, Chief Technology Officer, IP Services
- Mel Bartels, Information Technology Manager, Organic Materials Review Institute
- Rudy Venturi, Network Administrator, United Way of Lane County
- Matt Barton, Chief Information Officer, Eugene Water and Electric Board
- Scott Noble, Sr. Programmer & Systems Analyst, Lane County Information Services
- Jeff Jones, Director of Identity and Directory Services, UO Information Services
- Barrett Avery, Software Engineer, IDX, LLC
- Aaron Martins, Software Engineer, SheerID
- Joe Maruschak, Executive Director, RAIN Eugene
- Mari Good, LCC CIT Faculty, Computer Programming
- Brian Bird, LCC CIT Faculty, Computer Programming
- Jim Bailey, LCC CIT Faculty, Computer Simulation / Game Dev. & CS Transfer
- Paul Wilkins, LCC CIT Faculty, Computer Simulation / Game Dev. & CS Transfer
- Joseph Colton, LCC CIT Faculty, Computer Network Operations
- Don Easton, LCC CIT Faculty, Computer Network Operations
- Pam Farr, LCC CIT Faculty, Database Specialist Cert.

- Chris Rehn, LCC Dean, Business & Computer Information Technology Division
- Gerry Meenaghan, LCC Cooperative Education Coordinator, CIT
- Callie Dedore, LCC CIT Student Member, AAS in Computer Programming

Program Summary/Description

Give a brief overview of the program including purpose, primary student audience, occupational/career preparation objectives; opportunities for continued or related training; other key features and highlights of the program.

This degree is an AAS degree program that prepares students with the knowledge and applicable skills necessary for entry-level careers in cybersecurity. Students will acquire foundational knowledge in computer science and information technology, in order to build solution-oriented skills in infrastructure security, enterprise risk and risk management, cloud computing, cryptography, information assurance, digital forensics, penetration testing and business continuity. Students will apply this knowledge both in a hands-on lab curriculum and through required internships supporting the local community. In addition, this degree will provide the core foundational knowledge to continue on to a bachelor's degree in cybersecurity and related areas for even further opportunities for career advancement.

Program Learning Outcomes

Upon successful completion of this program, students will know or be able to:

- Defend systems against unauthorized access, modification and/or destruction
- Perform vulnerability and networking scanning assessments
- Monitor network traffic for unusual activity
- Configure and support security tools such as firewalls, anti-virus software, patch management systems, etc.
- Implement network security policies, application security, access control and corporate data safeguards
- Analyze and establish security requirements for your networks
- Train fellow employees in security awareness and procedures
- Develop and update business continuity and disaster recovery protocols
- Conduct security audits and make policy recommendations
- Gain fundamental knowledge of key compliance frameworks
- Provide technical security advice

Core Learning Outcomes

To which Lane Core Learning Outcomes dimensions does this program align? Example: CLO 1.2: Determine information need, find and cite relevant information. Learn more about Core Learning Outcomes and curriculum mapping. For help, contact the Coordinator of Student Learning Assessment and Curriculum Development.

- **CLO 1**: Think critically
  - 1.2 Determine information need, find and cite relevant information
- **CLO 3**: Create ideas and solutions
  - 1.2 Experiment with possibilities that move beyond traditional ideas or solutions. Embrace ambiguity and risk mistakes
- **CLO 5**: Apply learning
  - 5.1 Connect theory and practice to develop skills, deepen understanding of fields of study and broaden perspectives
  - 5.2 Apply skills, abilities, theories or methodologies gained in one situation to new situations to solve problems or explore issues

Proposed Curriculum

List courses by year (e.g., Year 1 or Year 2) and term (Fall, Winter, Spring, Summer). Add rows as needed. Please put courses in the order in which students should take them. Provide accurate course information. Add rows as needed.

1 lecture credit = 1 contact hour
1 lecture/lab credit = 2 contact hours
1 lab credit = 3 contact hours

Describe/list Program Prerequisites (if applicable):

Year/Term	Course Subj/No.	Course Title	Credits	Contact/ Clock Hours Per Week
1st year/Fall	CIS 100	Computing Careers Exploration	1	1 lecture
1st year/Fall	CS 179	Introduction to Computer Networks	4	3 lecture, 3 lab
1st year/Fall	MTH 111	College Algebra	5	5 lecture
1st year/Fall	CIS 140W	Introduction to Operating Systems: Windows Clients	4	2 lecture, 3 lab, 2 lecture/lab
1st year/Winter	CS 240W	Advanced Windows: Server Management	4	2 lecture, 3 lab, 2 lecture/lab
1st	CS 161C+	Computer Science 1	4	2 lecture, 4

year/Winter				lecture/lab
1st year/Winter	CS 206	Co-op Ed: Computer Information Technology Seminar	2	2 lecture
1st year/Winter	PE	PE/Health Requirement	3	9 lab
1st year/Winter	CS 189	Routing and Switching Essentials	4	2 lecture, 3 lab, 2 lecture/lab
1st year/Spring	CG 203	Human Relations at Work	3	3 lecture
1st year/Spring	CS 162C+	Computer Science 2	4	2 lecture, 4 lecture/lab
1st year/Spring	CS 273	Intro to Cloud Computing	4	2 lecture, 4 lecture/lab
1st year/Spring	WR 121	Academic Composition	4	4 lecture
2nd Year/Fall	CS 260	Data Structures 1	4	2 lecture, 4 lecture/lab
2nd Year/Fall	CIS 140U	Introduction to Unix/Linux	4	2 lecture, 3 lab, 2 lecture/lab
2nd Year/Fall	CS 284	Network Security Fundamentals	4	2 lecture, 3 lab, 2 lecture/lab
2nd Year/Fall	CS 188	Wireless Networking	4	2 lecture, 3 lab, 2 lecture/lab
2nd Year/Winter	Elective	Math above 111 or any CS/CIS above CS 120	4-5	?
2nd Year/Winter	WR 227	Technical Writing	4	4 lecture
2nd Year/Winter	CS 240U	Advanced Unix/Linux: Server Management..	4	2 lecture, 3 lab, 2 lecture/lab
2nd Year/Winter	CIS 125D	Software Tools 1: Databases	4	2 lecture, 3 lab, 2

				lecture/lab
2nd Year/Spring	CS 280 CN	Co-op Ed: Computer Network Operations	3	9 lab
2nd Year/Spring	CS 285	Cybersecurity Operations	4	2 lecture, 3 lab, 2 lecture/lab
2nd Year/Spring	CS 286	Firewalls and VPNs	4	2 lecture, 3 lab, 2 lecture/lab
2nd Year/Spring	CS 288	Network Monitoring and Management	4	3 lecture, 3 lab
Total Program Credits			93-94	

Signatures

Primary Program Faculty/Coordinator

Name: Don Easton
Signature:
Date: 19 Nov 2018

Division Dean

Name: Christopher Rehn
Division: BCIT
Signature:
Date: 11/19/18

VP for Academic and Student Affairs

Name:
Signature:
Date:

Program Research/Evidence

To be completed by faculty and dean prior to developing the Program Proposal Application.

Considerations

Begin program[1] research by considering end goals and outcomes for students. What will students know or be able to do at the end of the program? What skills and knowledge are required? What career and transfer opportunities are there? Who are the stakeholders and collaborators? Please provide evidence.

Note: Career Pathway Certificates (CPC) are 12-44 credits and generally do not require the same level of research as larger certificates and degrees. For help developing a CPC, please contact the Career Pathways office.

Program Title

Cybersecurity (AAS)

Describe Program Need (State Standard A)

Provide clear evidence of the purpose this program serves at Lane and in the community. Determine/identify the following:

- Regional/state labor market and employment demand
- Projected employment and future employment trends
- Wages and wage progression (include starting wages)
    - Average starting wages
    - Average wages
- List job titles related to this program
- Career pathways and educational pathways
- Include links to labor market information from state and federal resources

We need to preface the following information with the statement that BLS/Oregon Employment Department do not have the exact job classification the students that complete this program will be qualified for (classification system appears to be somewhat antiquated). The role of the security administrator/security specialist does exist and is in demand, as the cybersecurity field has different levels of jobs and each serves a specific purpose or purposes. Information technology career paths faced the same problems a couple of decades ago, but has evolved into a field with many different roles available. With that said, some data is an estimate based on comparison between the information security analyst (higher level) and network/systems

---

[1] "Programs" in this context refers to career-technical degrees (Associates of Applied Science, AAS) and Certificates of Completion.

administrator (equivalent classification on the information technology side).

- Regional/state labor market and employment demand –
  - This occupation is expected to grow at a much faster rate than the statewide average growth rate for all occupations through 2027.
  - Nationwide, there were over 100,000 openings in 2016 alone
- Projected employment and future employment trends
  - Growth is above average
    - National – 28% over the next 10 years
    - Willamette Valley – 16% over the next 10 years

- Wages and wage progression (include starting wages)
  - Average starting wages
    - National - $45.92 per hour
    - Willamette Valley - $ 26.54 per hour
  - Average wages (Median)
    - National - $45.92 per hour
    - Willamette Valley - $34.58 per hour
- List job titles related to this program
  - Security Administrator
  - Systems Security Administrator
  - Network Security Administrator
  - IT Security Specialist
- Career pathways and educational pathways
  - Career pathways include roles that can lead to progressively more advanced roles
  - Educational pathways can lead to industry certifications, specialized training, transfer to a four year program, and graduate school
- Include links to labor market information from state and federal resources
  - Federal
    - https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
    - https://www.bls.gov/ooh/computer-and-information-technology/network-and-computer-systems-administrators.htm#tab-8
  - State
    - https://www.qualityinfo.org/jc-oprof/?at=1&t1=information%20security~151122~4101000000~0~true~true~true~true~true~true~true~true~true~true~true~true~none~0~1~1
    - https://www.qualityinfo.org/jc-oprof/?at=1&t1=information%20security~151142~4101000000~0~true~true~true~true~true~true~true~true~true~true~true~true~none~0~1~1

Describe Program Collaboration (State Standard B)

Describe collaboration with relevant stakeholders and college departments.

We have been collaborating with a variety of stakeholders, both internal and external of the college. Internally, we have been working closely with the Curriculum Development office to ensure all information is being collected and documented correctly. Other faculty within CIT

have been engaged and are active advisors during the development process and will continue after degree approval. Cooperative education has been a strong partner through this process, providing much need consultation and assistance in determining program relevance and industry support for internship and employment opportunities.

Externally, we have engaged with the CIT Advisory Board and other local businesses in order to gather valuable input and support. We conducted a survey to gather feedback from the Advisory Board and other local businesses and received excellent feedback about the proposed degree program. The participants are composed of representatives of organizations that employ our graduates, so their input is especially critical to this process.

Describe Program Alignment (State Standard C)

Describe regional educational alignment and workforce development. Identify career ladders, stackable credentials, and education (transfer) and training opportunities. Describe alignment with Lane mission, vision, and four Core Themes. For Career Pathway Certificates: describe how this new CPC fits into an AAS degree or other Certificate of Completion. Is this Entry Level or Advanced? (See information about CPCs here)

The proposed AAS in Cybersecurity aligns with Lane's vision, mission, and core themes. It is designed to provide a quality learning centered experience that promotes the success of our students.

Core Theme 1: Responsive Community Engagement:

CIT has an advisory board made of representatives from various industries in the local area. When surveyed, there was a positive affirmation that internship opportunities will be available for students in this program. In working with cooperative education, there have been requests within the last academic year for students interested in cybersecurity internships from local companies, which reinforces that opportunities will be available.

Core Theme 2: Accessible and Equitable Learning Opportunities:

This program supports the college's efforts to introduce and support equity in all curriculum. Access to the program will be designed in such a way to be inclusive of all, recognizing that all students have something to contribute. Materials will be made available in alternate formats (where feasible) to ensure that students have equal access. Materials will be produced in such a way to encourage women, minorities, and people with disabilities to consider occupations within cybersecurity.

Core Theme 3: Quality Educational Environment:

This program is unique in the Willamette Valley. It provides a career path in cybersecurity, which fills a critical gap in the local community. Our programs have continuously met the needs of the local area by providing them with a pool of candidates that are exceptional. Through our stringent program review process, we are constantly striving to improve and update programs to maintain relevancy and currency with the changing workplace. We have implemented many innovative learning tools and modern technology into our programs in CIT, with the goal of

creating an environment that encourages collaboration and provides flexibility to provide a quality learning environment that meets the different ways in which our students learn.

Core Theme 4: Individual Student Achievement:

Our graduates enter the workplace as valued employees. Graduates are also prepared to move on to meet any additional educational goals they may have at the university level. Cybersecurity is a field that requires a person to always learn. Technological changes, both attack and defense, require consistent research and training. Because of this, the AAS provides a solid foundation that prepares the graduate to be prepared to enter the workplace and simultaneously continue their education to progress in the field.

Stackable credentials:

The next logical step is create additional CPCs to provide targeted skill development and to compliment other degree programs within CIT where students are looking to develop specializations.

Program Design (State Standard D)

Identify and describe the knowledge, skills, and competencies relevant for this program. Preliminary program design should include: Evidence of local/regional opportunities for co-op, internships, work study (e-mail or written documentation from co-op coordinators and/or employers verifying available opportunities). Include a program description and learning outcomes.

Program Description

This degree is an AAS degree program that prepares students with the knowledge and applicable skills necessary for entry-level careers in cybersecurity. Students will acquire foundational knowledge in computer science and information technology, in order to build solution-oriented skills in infrastructure security, enterprise risk and risk management, cloud computing, cryptography, information assurance, digital forensics, penetration testing and business continuity. Students will apply this knowledge both in a hands-on lab curriculum and through required internships supporting the local community. In addition, this degree will provide the core foundational computer science knowledge to continue on to a bachelor's degree in cybersecurity and related areas for even further opportunities for career advancement.

(Note: This is not just another IT degree. This degree is designed to produce knowledgeable security administrators that are proficient in many of the core areas of cybersecurity. This is the 'boots on the ground' person who can handle routine tasks, freeing more experienced personnel to focus on advanced tasks, yet is capable in situations where their knowledge places them above their peers within IT.)

Program Outcomes[2]

By the end of this program, students should know and/or be able to:

- Defend systems against unauthorized access, modification and/or destruction
- Perform vulnerability and networking scanning assessments
- Monitor network traffic for unusual activity
- Configure and support security tools such as firewalls, anti-virus software, patch management systems, etc.
- Implement network security policies, application security, access control and corporate data safeguards
- Analyze and establish security requirements for networks
- Train fellow employees in security awareness and procedures
- Develop and update business continuity and disaster recovery protocols
- Conduct security audits and make policy recommendations
- Provide technical security advice

Evidence of opportunities for co-op, internships

As mentioned above, we have engaged with the CIT Advisory Board in order to gather valuable input and support. We conducted a survey to gather feedback about the proposed degree program from the Advisory Board and received excellent feedback that was overwhelmingly positive. Since the advisory board is composed of representatives of organizations that employ our graduates, their input is critical to this process. Many local companies have confirmed they would like to provide internships. Also, many of these same businesses said they planned on hiring at the two-year education level in the coming years. These are the same companies that consistently hire graduates from existing CIT programs.

Indicate Evidence of Program Capacity (State Standard E)

(This section not required for Career Pathway Certificates)

"*The college must have the resources to offer the proposed program without negatively impacting existing approved programs*" (Higher Education Coordinating Commission, HECC Approval Standards, 2014)

Provide evidence of the resources (personnel, financial feasibility, facilities, instructional, marketing, etc.) available or needed to develop, implement, and sustain the program. How will you recruit students; who is your target student population? To complete this section, collaborate with partners such as: the library, budget office, co-op coordinators, facilities, and others who can help determine resource availability and needs.

No additional resources will be necessary, beyond what is currently available to support other programs within the department. Course development will be minimal, as many of the courses in the proposed degree program are already available. Any additional course development will be performed by assigned faculty in the course of their normal duties. The target student population will include recent high school graduates, veterans, underrepresented groups, and those interested in a career change or retraining. Students will be recruited through normal

---

[2] Developing learning outcomes: https://www.lanecc.edu/assessment/developing-and-refining-learning-outcomes

outreach efforts that the college utilizes. There is also a high school outreach effort that is gaining momentum, which is designed to inform students about the career options within cybersecurity. It is critical to get young people interested in the field as they are the next generation to protect our digital world.

Resources

- Community Colleges and Workforce Development (CCWD). (2015). Higher Education Coordinating Commission approval standards. *Oregon Community Colleges Handbook & Planning Guide, 2015 Edition.*
- Lane Core Themes (CT)
    - CT1: Responsive Community Engagement
    - CT2: Accessible and Equitable Learning Opportunities
    - CT3: Quality Educational Environment
    - CT4: Individual Student Achievement
- Lane Vision, Mission, and Values
- State of Oregon Employment Department
- U.S. Department of Labor, Bureau of Labor Statistics: Occupational Outlook Handbook

---

Signatures

Primary Program Faculty/Coordinator

Name: Don Easton

Signature

Date: 19 NOV 2018

Division Dean

Name: Chris Rehn

Division: BCIT

Signature

Date: 11/19/18

Labor Market Information Worksheet

Fill out the labor market information for Associate of Applied Science and independent Certificate of Completion programs only.

Program Title	**AAS Cybersecurity**
Classification of Instructional Programs* family and number Example: 13) Education, 13.1001) Special Education and Teaching, General	**11.1003) Computer and Information Systems Security/Information Assurance**

Use this website to determine CIP code*: https://nces.ed.gov/ipeds/cipcode/Default.aspx?y=55

What are the common job titles for the occupations that use the skills your program will teach?

- Systems Security Administrator
- Network Security Administrator
- IT Security Administrator

What occupational title(s) most closely describes the above occupations?

Occupational Title	Region
Security Administrator	Global
Network Security Administrator	Global
IT Security Specialist	Global

Is a license required by the state of Oregon to perform this occupation?

If yes, how many licenses were held in the most recent year?

No

What are the potential career ladder, steps, or career pathway for program completers?

There is a strong pipeline for graduates of a 2-year program in cybersecurity. This level of training and on-the-job experience can lead a student in a variety of different directions. The most linear path is to continue their education, whether academic or professional, while gaining new skills and expanding on

existing ones. Generally, someone in this field would begin as a security administrator, progress to security analyst, then to security engineer. Of course, this is the purely technical track. Graduates could branch out to supervisory roles or into complementary roles where the skills they have developed provide significant benefit. For example, a security administrator is promoted into a security analyst position. Security analysts often work with risk management, so a potential career path could lead them into fiscal compliance or human resources.

What are the minimum educational requirements for these jobs?

Associate-level education with industry certifications

Is training available for related career ladder/pathway occupation(s) and at what types of institutions?

Yes. Further training can be obtained at 4-year universities, private training centers, web-based training subscriptions, and on-the-job training.

Please describe any other labor market information that may be relevant to this program

It was difficult to find exact matches when evaluating the targeted job role this degree is focused on. Since this specialization is still relatively new, below are links to BLS and State of Oregon information:

https://www.bls.gov/oes/current/oes151122.htm

https://www.qualityinfo.org/jc-oprof/?at=1&t1=information%20security~151122~4101000000~0~true~true~true~true~true~true~true~true~true~true~true~true~true~none~0~1~1

Resources

- State of Oregon Employment Department
- U.S. Department of Labor, Bureau of Labor Statistics: Occupational Outlook Handbook

Signatures

Primary Program Faculty/Coordinator

Name: Don Eastoy
Signature:
Date: 19 Nov 2018

Division Dean

Name: Chris Rehn
Division: BCIT
Signature:
Date: 11/19/18