PENINSULA COLLEGE

Degree Guide:

Cybersecurity and Computer Forensics, Associate in Applied Science-Transfer (AAS-T) Degree

Program
Cybersecurity & Computer Forensics (CSIA)
Degree Type
Professional Technical Degree
Program Coordinator

Alex Markunas
(360) 417-6270
amarkunas@pencol.edu

Program Description

Increased cybersecurity threats and new homeland security policies have produced a growing national demand for cybersecurity professionals with knowledge of cybersecurity, ethical hacking, intrusion testing, vulnerability assessment, and computer forensics. In addition, the growth of universal and mobile computing require new approaches to information security and the protection of information systems from unauthorized access, modification, or destruction. The Cybersecurity and Computer Forensics program prepares students for entry level employment in cybersecurity and computer forensics careers including cyber incident and response, vulnerability detection and assessment analyst, computer forensic analyst, and computer forensics investigator. Foundation courses introduce students to the legal, ethical, and theoretical issues in cybersecurity and computer forensics technology. Core courses expand student depth and skills in ethical hacking, criminal justice, evidentiary analysis, and the development of a forensically sound environment. Capstone courses provide practicum experience and opportunity to participate in the Collegiate Cyber Defense Competition (CCDC). Successful completion of this program leads to an Associate in Applied Science-Transfer (AAS-T) degree Cybersecurity and Computer Forensics. Students are required to have access to computer, internet, and browser.

*Note: CS& 141, CS 142, MATH& 141, MATH& 142, MATH& 151, and ENGL& 102 are required for transfer to Western Washington University. Students should work with the Cybersecurity Program Advisor to ensure transfer requirements are met.

Program Length: 6 Quarters
Program Code: CISCCAAS

Career Opportunities and Earnings

There is a high demand for talented people with cybersecurity skills; and an increasing number of employers are seeking workers with knowledge of computer forensics tool. Graduates may find positions with a variety of critical infrastructure companies and organizations in the public and private sectors. Some employers may require employee background checks.

- Computer forensic analyst
- Cybersecurity specialist
- Incident responder
- Information security analyst
- Security monitoring and event analysis
- System and network penetration tester

For current employment and wage estimates, please visit and search for the relevant occupational term: bls.gov/

oes.

Program Outcomes

When this program is completed, the student will be able to:

- Demonstrate an understanding of the core concepts, tools, and methods used to secure computer systems
- Identify and present indicators that a cybersecurity incident has occurred
- Apply criminal justice methods to cybersecurity and computer forensic investigations
- Plan, implement, and evaluate penetration testing and ethical hacking of computer systems
- Identify, analyze, and mitigate threats to internal computer systems
- Collect, process, analyze, and present computer forensic evidence
- Work in teams to analyze and resolve cybersecurity issues
- Apply critical thinking skills to risk analysis of computer systems

Special Features

- The program encourages students to explore the legal, ethical, and global impact of cybercrime on private, public, and personal computing infrastructures
- The courses are based on the CNSSI standards established by the U.S. National Security Agency (NSA) for training information systems security professionals
- The program provides up to date curriculum that adapts to the rapidly changing field of cybersecurity and computer forensics
- The Peninsula College Cybersecurity and Computer Forensics program is significantly more cost effective than most private and public schools

Approximate Additional Costs

- Books, supplies and miscellaneous fees (per quarter): $200 - $250

Sample Schedule

This sample schedule is provided as a guide for a full-time student starting in fall quarter whose goal is to earn the AAS-T. The typical student schedule is based on entering the program during the fall quarter, however some programs allow students to enter in the winter or spring as well. Since not all do, please confirm with an advisor whether this program must be started during a specific quarter or not.

First Quarter (Fall)

Catalog #	Course Title	Credits
CS 100	Introduction to Computer Science	5
IT 107 or IT 111		5
MATH& 141	Precalculus I	5

Second Quarter (Winter)

Catalog #	Course Title	Credits
IT 155 or IT 211		5
IT 260	Introduction to Unix/Linux Systems Administration	5
MATH& 142	Precalculus II	5

Third Quarter (Spring)

Catalog #	Course Title	Credits
CSIA 110	Introduction to Cybersecurity and Cybercrime	5
IT 114	Database Design and Implementation	5
MATH& 151	Calculus I	5

Fourth Quarter (Fall)

Catalog #	Course Title	Credits
CSIA 195	Cybersecurity III: Ethical Hacking	5
ENGL& 101	English Composition I	5
IT 207, IT 275 or IT 285		5

Fifth Quarter (Winter)

Catalog #	Course Title	Credits
CS& 141	Computer Science I with Java	5
ENGL& 102	Composition II	5
SOCSI 101	Contemporary Global Issues	5

Sixth Quarter (Spring)

Catalog #	Course Title	Credits
CS 142	Computer Science II with Java	5
CSIA 290	Cybersecurity Capstone	5
PSYC& 100	General Psychology	5

Your personal educational plan will vary based on many factors including:

- The quarter you begin
- How many classes/credits you plan to take in each quarter
- Your math and English placement; Learn more about placement options by visiting the Assessment and Placement website.
- If you start in our Transitional Studies program

Total Credits	**90**