PUGET SOUND SKILLS CENTER

Cybersecurity Academy
September 6, 2024

Course Description:
The Cybersecurity Academy at Puget Sound Skill Center is a comprehensive program designed to prepare students for careers in cybersecurity. Through hands-on labs, real-world simulations, and industry-aligned instruction, students will develop the skills needed to protect systems, networks, and data from digital threats. The program covers a range of topics, including network security, ethical hacking, cryptography, and cybersecurity policies. Students will be eligible to take industry-recognized certifications such as CompTIA Security+, Network+, and Certified Ethical Hacker (CEH).

Culture of Learning:
We foster a culture of responsibility and vigilance in our classroom, essential traits for any cybersecurity professional. The course will be highly interactive and collaborative, with a focus on problem-solving and critical thinking. Attendance and active participation are critical as students will be working in teams on real-world cybersecurity challenges. Materials will be posted in our Google Classroom, and grades will be updated regularly. The program includes a practical component where students will engage in cybersecurity simulations and internships with industry partners.

This course reinforces PSSC's school-wide agreements: Be Present, Be Respectful, Be Engaged, and Be Professional. Each cybersecurity classroom will also develop specific behavior agreements to ensure a safe and productive learning environment. These agreements will be supported through a progressive system including individual check-ins, positive reinforcement, and, if necessary, interventions from the Dean or Counselor.

Student Learning Outcomes:

Cybersecurity Skills Mastered:

- Protecting networks and systems from cyber threats
- Ethical hacking and penetration testing
- Network configuration and management
- Implementing security policies and procedures
- Cryptography and data protection
- Incident response and disaster recovery
- Security risk assessment and management
- Understanding and applying cybersecurity laws and regulations
- Collaboration with IT teams to secure infrastructure
- Preparation for CompTIA Security+, Network+, and CEH certifications

Standards Assessed:

- **1.B.2** Be open and responsive to new and diverse perspectives; incorporate group input and feedback into the work.

- **2.C.4** Interpret information and draw conclusions based on the best analysis.
- **3.A.1** Articulate thoughts and ideas effectively using oral, written, and nonverbal communication skills in a variety of forms and contexts.
- **3.B.1** Demonstrate ability to work effectively and respectfully with diverse teams.
- **6.A.1** Use technology as a tool to research, organize, evaluate, and communicate information.
- **10.A.1** Set and meet goals, even in the face of obstacles and competing pressures.
- **11.A.1** Use interpersonal and problem-solving skills to influence and guide others toward a goal.
- **11.B.1** Act responsibly with the interests of the larger community in mind.

Instructor Contact Information:
Peller Phillips
Email: Peller.phillip@highlineschools.org
Phone: 786-363-7314 (call or text)

Credits Offered:

- **Credits per Semester:** 1.5 high school credits per semester
- **Equivalency Credits:** 0.5 Technology, 1.0 Elective
- **College Credits:** Bellevue College - Cybersecurity 101: Introduction to Cybersecurity - 4 credits

Industry-Recognized Certifications:

- CompTIA Security+
- CompTIA Network+
- Certified Ethical Hacker (CEH)

Grading Policies:
We use Standards-Based Grading to assess student learning as per Highline Public Schools.

The grade scale is as follows:

- **4 (A; 3.2 - 4.0): EXCEEDING STANDARD**
- **3 (B; 2.4 - 3.19): MEETING STANDARD**
- **2 (C; 1.6 - 2.39): APPROACHING STANDARD**
- **1 (D; 1.2 - 1.59): BEGINNING**
- **NC (NC; 0 - 1.19): NO EVIDENCE/NO CREDIT**

Reassessment Opportunities:
Reassessment opportunities will be clearly published and determined by the instructor. Not all assignments and assessments are eligible for reassessment. The instructor will clearly communicate what is and is not reassessible. Reassessment opportunities will be within the unit. After a unit has closed, reassessment will not be available.

Professional Attire & Uniform Requirements:
Students must wear a lanyard with their student ID and PSSC-provided attire and/or program-specific uniform as required by the instructor. Dress should be professional, suitable for a cybersecurity professional attending industry events or working in an IT environment.

Course Technology:
This course utilizes Google Classroom.

- **AM Course Code:** qlsbad5
- **PM Course Code:** 2w6odiy

Work-Based Learning (WBL):
WBL is an instructional strategy that provides students with career exploration opportunities and hands-on learning where knowledge gained in CTE courses can be applied to real-life work experiences. The goal of every work-based learning program is to prepare students for the next generation of the workforce. PSSC students will participate in Work-Based Learning through their cybersecurity program and may earn elective credits.

Common WBL opportunities include:

- Internships with cybersecurity firms
- Participation in Cybersecurity Competitions
- Job shadowing with IT security professionals

All PSSC students will participate in Work-Based Learning.

Leadership:
Leadership is a key component of the Cybersecurity Academy, where your student can be a member of the Cybersecurity Club. The purpose of this club is to foster leadership qualities, social awareness, and a sense of responsibility in the digital world. Students can engage in activities such as cyber defense competitions, community outreach on cybersecurity awareness, and leadership roles within the program.

List of opportunities:

- Cybersecurity competitions and conferences
- Community Service related to digital literacy and cybersecurity
- PSSC Program Leadership

Cell Phone Policy:
Cell phones should be used for educational purposes only as directed by the instructor.

Attendance Policy:
The seat time mandate for CTE courses in Washington ensures students receive sufficient instructional hours and hands-on training time to master necessary technical skills. Prescribed minimum seat time safeguards the quality of CTE programs by allowing for in-depth classroom learning, adequate lab practice on equipment, and fulfillment of certification requirements. Upholding seat time standards is crucial for preparing a workforce with job-ready expertise meeting industry needs.

Therefore, it is critical that students are present. Whether excused or unexcused, missed time is missed time.

1. If a student is tardy, they must complete the QR code in their classroom. It is their responsibility as a student to complete the QR code so their absence can be corrected to a tardy. If they do not complete the QR code, the student will be marked absent.

2. As a professional courtesy, please contact the course instructor via email, Google Voice text, or phone call.

3. Absences may be excused by any of the following methods within 48 hours of the absence:

- Phone call to PSSC Attendance Specialist Kelsey Gomez (206-631-7353)
- Email to PSSC Attendance Specialist Kelsey Gomez (kelsey.gomez@highlineschools.org)
- Hand-written note turned into PSSC Attendance Specialist Kesley Gomez

4. Please include the following information in the note, call, or email:

- Student Name
- Parent Name
- Date of the absence
- Reason for the absence

5. Prearranged absence forms are in the office. The form must be completed with all required signatures before the departure date. This form will be shared with your home school as well.
6. Reassessment opportunities will be published and determined by the instructor. Not all assignments and assessments are eligible for reassessment.

Student Handbook: CLICK HERE TO VIEW

Year 2 Eligibility:
All Year 1 PSSC students will have quarterly check-ins with their PSSC teachers, student success dean, counselor, and families to assess performance in their program, needed supports, and progress towards mastery of content and skills necessary for Year 2 programming. All information will be shared with the home school support staff.

Course Student Outcomes:

- Apply knowledge of cybersecurity principles to protect networks and systems from digital threats.
- Analyze and address vulnerabilities within IT systems.
- Understand the ethical implications of cybersecurity practices.
- Develop and implement security policies in a simulated environment.
- Prepare for industry-recognized certifications in cybersecurity.

Required Assessments:
All assignments in our PSSC Cybersecurity Academy course contribute to students' grades for CWU college credit. There are two required assessments to earn credit from CWU: a Capstone Project in Cybersecurity and a Final Reflection Paper.

CWU Grade Scale:

A A-	4.0 3.7	Excellent	Meets all objectives of the course and fulfills all requirements; performs at a level that reflects excellence

B+ B B-	3.3 3.0 2.7	Good	Meets all objectives of the course and fulfills all requirements; performs at a high level
C+ C C-	2.3 2.0 1.7	Satisfactory	Meets all objectives of the course and fulfills all requirements; performs at a satisfactory level
D+ D D-	1.3 1.0 0.7	Marginal Pass	Makes progress toward meeting the course objectives; fulfills course requirements at a substandard level
F	0	Failure	Fails to meet the course objectives; does not fulfill course requirements