Career-Technical Credit Transfer (CT)²
Cybersecurity Career-Technical Assurance Guide (CTAG)
April 12, 2019

The following course, indicated by a Career-Technical Articulation Number (CTAN), is eligible for post-secondary credit and transfer among Ohio's public institutions of higher education. The SCTAI alignment document with ODE competencies and post-secondary learning outcomes can be found on the ODHE website at https://www.ohiohighered.org/transfer/ct2/ctags.

CTCYBR001 - Cybersecurity Fundamentals	**Credits: 3 Semester Hours**
Advising Notes: To access post-secondary college credit for this CTAN, the student must: • Matriculate to an institution of higher education with an approved or comparable program within 3 years after completing the approved secondary program • Successfully complete ODE secondary course **Cybersecurity Defense and Reinforcement (146010)** and earn a qualifying score of ***60 or higher*** on the corresponding End of Course examination	Secondary institutions must have pathway approval from the Ohio Department of Education. Certificate of Affirmation assurances are now incorporated into the CTE-26 application process.

The CTAN identifies learning outcomes that are equivalent or common in introductory technical courses. For students to receive credit under these agreements, the career-technical secondary programs and the post-secondary institutions must document that their course content matches the learning outcomes in the CTAN.

Requirements and Credit Conditions:

1. The receiving institution must have a comparable program, major, or course that has been approved through submission to the Ohio Department of Higher Education (CT) [2] approval process for the CTAN listed in this document.
2. Credits apply to courses in the specified technical area at Ohio's public institutions of higher education, if the institution offers courses in the specific technical area. In the absence of an equivalent course, and when the institution offers the technical program, the receiving institution will guarantee to grant and apply an equivalent credit value of the Career-Technical Articulation Number (CTAN) toward the technical requirements of the specific degree/certificate program.
3. The applicant must provide proof to the receiving institution that she/he completed a course that has been approved through the (CT)² approval process and that she/he has passed the end-of-course assessment.
4. A career-technical student seeking credit under the terms of this CTAG must apply and be accepted to the college within three years of completing a career-technical course.
5. A career-technical student who meets all eligibility criteria will receive the credit hour value for the comparable course as offered at the receiving state institution of higher education.
6. The admission requirements of individual institutions and/or programs are unaffected by the implementation of (CT)² outcomes.
7. The transfer of credit, through this CTAG, will not exempt a student from the residency requirements at the receiving institution.

Secondary Career-Technical students must complete the ODE course "Cybersecurity Fundamentals" to be eligible for credit under this CTAG. This pathway is outlined in the Ohio Department of Education's *Information Technology Career Field Technical Content Standards*.

CTCYBR001 - Cybersecurity Fundamentals	**Credits: 3 Semester Hours**

General Course Description: This course will provide the student with basic knowledge of cybersecurity dynamics and is the entry point for students desiring to major in Computer Security Systems. The course will address issues involving hackers, malware, social theories, protocols, firewalls, and intrusion detection. In addition, this course will discuss the prevention and containment of intrusion incidents, the incident response process, and the forensic examination of a computer.

Credits: 3 Semester Hours

Learning Outcomes:

1. *Discuss the social theories of computer-enabled abuse and the role of compliance framework in mitigating abuse.
2. *Discuss the malicious user's motivation such as social engineering and cyber warfare.
3. *Explain worms, trojans, viruses, spyware, ransomware other types of malicious software.
4. *Demonstrate an understanding of how encryption can be used and abused (such as Public Key, cryptography, symmetric cryptography, algorithm length, escrow, key recover, key splitting, random number generator, nonce, initialization vector, cryptographic mode, plaintext, cipher text, S/MIME, PGP, IPsec, TLS).
5. *Describe standard communication protocols associated with cybersecurity.
6. *Categorize various types of network and computer attacks and the actors that might perform them (potential system attacks, MITM attacks, DOS attacks, black hat attackers (nation states), etc.).
7. *Compare firewalls, intrusion detection, and intrusion prevention.
8. *Examine how information security can be used to mitigate cyber-crimes.
9. *Create a plan to defend against cyber-attacks.
10. *Formulate an incident response plan.

Asterisk Indicates Essential Learning Outcomes

Cybersecurity Panel Participants
April 2019

Dr. John Nicholas	University of Akron	Cybersecurity Lead Panel Expert
Dr. John Hoag	Ohio University	SCTAI Panel Expert
Kara Brown	Sinclair Community College	SCTAI Panel Expert
Glenn Goe	Stark State College	SCTAI Panel Expert
Doug Huber	Lorain County Community College	SCTAI Panel Expert
Dovel Myers	Shawnee State University	Item Writer
John Wiseman	Ohio Department of Education	Program Specialist
Anne Skuce	Ohio Department of Higher Education	Senior Associate Director, SCTAI