Approved Innovative Course

- *Districts must have local board approval to implement innovative courses*
- *Innovative courses may meet state elective credit only*
- *CTE Innovative courses may not be the final course in a coherent sequence used for an endorsement*
- *Course requirements must be met without modification*

Course: Principles of Cybersecurity
PEIMS Code: N1302810
Abbreviation: CYBRSEC
Grade Level(s): 9-12
Number of Credits: 1.0

Course description:

This course develops the knowledge and skills needed to master fundamental concepts of cybersecurity. Students in the course will develop a basic foundation for continuing their cybersecurity education and choosing a career in the cybersecurity field. Students will explore the challenges facing information security professionals related to ethics, system security, network security, and application security. Students will conduct risk assessments and develop and implement security policies to mitigate those risks. Students will examine trends in cyber-attacks, common vulnerabilities, and the emergence of cyber terrorism.

Essential knowledge and skills:

(a) General Requirements. This course is recommended for students in Grades 9-12

(b) Introduction.

(1) Career and technical education instruction provides content aligned with challenging academic standards and relevant technical knowledge and skills for students to further their education and succeed in current or emerging professions.

(2) The Information Technology (IT) Career Cluster focuses on building linkages in IT occupations for entry level, technical, and professional careers related to the design, development, support, and management of hardware, software, multimedia, and systems integration services.

(3) In the Principles of Cybersecurity, students will develop the knowledge and skills needed to master fundamental concepts of cybersecurity by exploring challenges facing information security professionals related to ethics, system security, network security, and application security. Students will examine trends in cyber-attacks, common vulnerabilities, and the emergence of cyber terrorism. Students will develop and implement security policies to mitigate those risks. To prepare for success,

students will have opportunities to apply, reinforce, and transfer knowledge and skills to a variety of settings and problems.

(4) Students are encouraged to participate in extended learning experiences such as career and technical student organizations and other leadership or extracurricular organizations.

(5) Statements that contain the word "including" reference content that must be mastered, while those containing the phrase "such as" are intended as possible illustrative examples.

(c) Knowledge and Skills.

(1) The student demonstrates necessary skills for career development and successful completion of course outcomes. The student is expected to:

(A) identify and demonstrate positive work behaviors such as regular attendance, punctuality, maintenance of a clean work environment, and professional written and spoken communication;

(B) identify and demonstrate positive personal qualities such as resilience, initiative, and a willingness to learn new knowledge and skills;

(C) employ effective reading and writing skills;

(D) solve problems and think critically;

(E) demonstrate leadership skills and function effectively as a team member; and

(F) demonstrate an understanding of ethical and legal responsibilities in relation to the field of information technology.

(2) The student identifies various employment opportunities and skill competitions in the cybersecurity field. The student is expected to:

(A) identify job opportunities and accompanying job duties and tasks;

(B) research careers in cybersecurity along with the education and job skills required for obtaining a job in cybersecurity in both the public and private sector;

(C) explain the functions of resumes and portfolios in the cybersecurity field;

(D) identify cybersecurity mental sports such as CyberPatriot, CyberLympics and Panoply; and

(E) identify and discuss cybersecurity certifications for cybersecurity related careers.

(3) The student understands current ethical and legal standards, rights and restrictions governing technology, technology systems, digital media and information technology, and the use of social media in the context of today's society. The student is expected to:

(A) demonstrate and advocate for ethical and legal behaviors both online and offline among peers, family, and community;

(B) identify and define unethical practices such as hacking, phishing, social engineering, online piracy, spoofing, and data vandalism;

(C) demonstrate ethical and legal behavior when confronted with usage dilemmas while using technology, technology systems, digital media, and information technology; and

(D) apply citation rules for various sources and mediums.

(4) The student understands and demonstrates the social responsibility of end users regarding the significant issues relating to digital technology and privacy, safety, and cyberbullying as it relates to cybersecurity. The student is expected to:

(A) identify and understand the nature and value of privacy;

(B) evaluate arguments related to the impact of emerging technologies on privacy;

(C) discuss the role of privacy in the student's lives and the impact of technology on the student's privacy;

(D) identify the importance of online identity management and monitoring;

(E) identify the signs, emotional effects, and the legal consequences of cyberbullying; and

(F) identify and discuss some effective ways to prevent, fight, and stop cyberbullying.

(5) The student identifies the consequences of practicing ethical hacking versus malicious hacking. The student is expected to:

(A) identify motivations for hacking;

(B) identify and describe the impact of cyber-attacks on the global economy, society, and individuals;

(C) distinguish between a cyber defender and a cyber attacker;

(D) differentiate types of hackers based on behaviors such as black-hats, white-hats, and gray-hats hackers;

(E) determine possible outcomes and legal ramifications of ethical versus malicious hacking practices; and

(F) debate whether it is ever appropriate to engage in ethical or malicious hacking practice.

(6) The student understands basic cybersecurity concepts and definitions. The student is expected to:

(A) define information security and cyber defense;

(B) identify basic risk management and risk assessment principles relating to cybersecurity threats and vulnerabilities;

(C) explain the fundamental concepts of Confidentiality, Integrity, and Availability also known as the CIA triad;

(D) identify and analyze current security concerns and recent cybersecurity breaches;

(E) define and discuss challenges faced by information security professionals;

(F) identify common risks, alerts, and warning signs of compromised computer and network systems;

(G) understand and explore the Internet of Things (IoT) and the vulnerability of network connected devices; and

(H) create an academic vocabulary using appropriate cybersecurity terminology.

(7) The student understands and defines hacking. The student is expected to:

(A) establish the proper definition of a hacker;

(B) identify commonly used hacking tools; and

(C) define vulnerability, exploit, port scanning, network sniffing, packet sniffing, and payload as they relate to hacking.

(8) The student identifies and defines cyber terrorism and counterterrorism. The student is expected to:

(A) define and explain counterterrorism;

(B) compare and contrast physical terrorism and cyber terrorism;

(C) construct standardized definitions of terrorism and cyber terrorism by interacting with multiple sources that provide examples and working definitions, including private and government agencies;

(D) identify the role of cyber defenders in protecting nations and corporations from physical and cyber terrorism, including hacktivism and state-sponsored terrorism;

(E) identify the role of cyber defense in 21st century society and global economy; and

(F) explain the importance of protecting important public infrastructures such as electrical power grids, public water, pipeline safety, railroads, sewer systems, and nuclear plants from cyber-attack.

(9) The student understands and explains various types of malicious software. The student is expected to:

(A) define malicious software;

(B) identify characteristics and traits of malicious software, including transmission and function;

(C) describe various types of malicious software, including Trojans, worms, and viruses;

(D) discuss how malicious software has shaped the global cybersecurity landscape and its future impact; and

(E) identify and critique delivery techniques for various types of malware such as spoofing, email attachment, and end user error.

(10) The student identifies methods for countering malicious software and protecting computer systems. The student is expected to:

(A) identify methods for manually and automatically removing malicious software from compromised computer systems, such as a virus or a trojan using anti-virus software or anti-malware programs;

(B) evaluate and compare free and commercial versions of the same antivirus software; and

(C) evaluate anti-malware programs for efficacy.

(11) The student understands information security vulnerabilities, threats, and computer attacks. The student is expected to:

(A) identify and define cyber-attacks and computer vulnerabilities;

(B) explore computer security vulnerabilities and different approaches to cybersecurity;

(C) explain how computer vulnerabilities leave systems open to cyber-attacks;

(D) identify emerging threats to computer systems due to programmer error as well as malicious hackers such as back door attacks;

(E) identify and differentiate attacks using malware;

(F) identify and differentiate different types of social engineering attacks such as shoulder surfing and dumpster diving;

(G) identify and classify various types of attacks on wireless systems; and

(H) identify various types of application specific attacks.

(12) The student understands, identifies, and explains the strategies and techniques of both ethical and malicious hackers. The student is expected to:

(A) identify internal and external threats to computer systems;

(B) identify and analyze different types of cyber-attack signatures;

(C) identify the capabilities of vulnerability assessment tools, including open source tools; and

(D) explain the concept of penetration testing, tools, and techniques.

(13) The student understands and demonstrates knowledge of system hardening techniques and strategies to prevent a computer system from being compromised by known vulnerabilities. The student is expected to:

(A) explain the importance of patched operating systems as it relates to securing a computer system;

(B) demonstrate basic use of system administration in control panel;

(C) activate and explain the importance of automatic updates;

(D) analyze and configure active and inactive services;

(E) explain the importance of creating a restore point and backup files; and

(F) research and understand best practices for securing computers, networks, and operating systems.

(14) The student demonstrates how to properly configure a computer network firewall. The student is expected to:

(A) identify and explain the basic function and purpose of network devices and technologies, including firewall and switches;

(B) analyze and establish incoming and outgoing rules for traffic passing through a computer network firewall;

(C) identify necessary and commonly used default ports and protocols according to number and service provided, such as Port 22 (ssh), Port 80 (http), and Port 443 (https);

(D) identify and block commonly exploited ports and protocols such as Port 21 (ftp) and Port 23 (telnet); and

(E) identify common tools for monitoring ports and network traffic.

(15) The student identifies best practices for creating secure local security policy. The student is expected to:

(A) establish secure password policy based on industry defined best practices;

(B) define what constitutes a complex and secure password;

(C) identify methods of attacking passwords, such as brute force and dictionary attacks;

(D) identify available user tools for the creation of complex secure passwords;

(E) implement a secure account lockout policy;

(F) analyze and correctly configure the audit policy of a computer to create event logs;

(G) analyze event logs for suspicious behavior; and

(H) examine and correctly configure the security options of a computer to ensure only authorized users have access.

(16) The student demonstrates necessary steps to maintain confidentiality and integrity of data on the computer system. The student is expected to:

(A) identify the different types of user accounts and groups on an operating system;

(B) establish policy to determine which users should have administrative rights on a computer system with role-based access control;

(C) explain the fundamental concepts and best practices related to authentication, authorization, and access control;

(D) identify multiple methods for authentication such as passwords, biometric verification, and security tokens;

(E) define and explain the purpose of an air-gapped computer;

(F) define and explain how checksums may be used to validate the integrity of transferred data;

(G) explain the importance of encrypting data to ensure integrity and to prevent unauthorized access; and

(H) identify applications commonly used to intercept data communication over wired and wireless networks.

(17) The student evaluates the potential risks and benefits of unsecured wireless networks. The student is expected to:

(A) identify the common risks associated with connecting portable devices to a variety of wireless networks such as public and home Wi-Fi;

(B) determine and evaluate the potential negative consequences of connecting a portable device to an unsecured wireless network;

(C) explain portable device vulnerabilities and wireless security solutions;

(D) compare WEP and WPA2 encryption;

(E) justify the purpose of broadcasting or hiding your wireless SSID; and

(F) research and discuss wireless attacks, including Bluetooth, MAC spoofing, war driving, eavesdropping, and man in the middle.

(18) The student analyzes common threats to computer applications. The student is expected to:

(A) define application security;

(B) identify methods of application security such as application development security, application hardening, and patch management;

(C) analyze web links in email, instant messaging, social media, and other online communication for spoofing or malicious links;

(D) demonstrate knowledge of pop-up and pop-under management;

(E) explain how users are the most common vehicle for compromising a system at the application level;

(F) demonstrate how to properly configure applications for automatic updates;

(G) research and explain ways to improve application security;

(H) identify web application vulnerability scanners and their function; and

(I) explain how coding errors can create vulnerabilities in the security of the application.

(19) The student explores possible exploits in mobile applications. The student is expected to:

(A) define rogue application and its use;

(B) explain how attackers are able to create rogue applications using reverse engineering;

(C) explain how changing the firmware to jail break a mobile devices can increase the potential for new exploits;

(D) describe how users often give mobile applications unnecessary permissions which facilitates fraudulent activities; and

(E) identify how client-side restrictions such as device security attributes, user location, and the security of the network connection can mitigate exploits on mobile devices.

(20) The student explores the field of computer forensics. The student is expected to:

(A) define computer forensics;

(B) explain the importance of computer forensics to law enforcement and corporations and its implications for individuals;

(C) identify and explain the four steps of the forensics process, including collection, examination, analysis, and reporting;

(D) identify under which circumstances a computer forensics investigation is necessary; and

(E) identify what types of information can be recovered in computer forensics investigations.

Description of specific student needs this course is designed to meet:

This course will provide students with an opportunity to develop valuable skills that will prepare them for cybersecurity jobs in the IT workforce, career pathway college readiness, and industry-recognized certifications. In addition, the course will provide students with:

- An understanding of ethical standards involved in cybersecurity
- Clear, commonly understood job descriptions and competency models
- An ability to assess the job market and their individual capability for success
- An understanding of training and education standards to develop technical skills
- An understanding of how to become the best talent for the cybersecurity workforce
- An ability to describe the career pathways, certifications, and college degrees required for professionals in the field

Major resources and materials:

Air Force Association. (2010). UNIT FOUR Principles of Cybersecurity. Retrieved December 2, 2015, from https://s3.amazonaws.com/cpvii/Training+materials/Unit+Four+-+Principles+of+Cybersecurity.pdf

American Board for Certification in Homeland Security. (2010). Digital forensics: An introduction. Retrieved December 2, 2015, from http://www.abchs.com/xsecure/chs/coursedocs/SSI_R1/pdf/DigitalForensics.pdf

INFOSEC. (2012, December 21). Cyberterrorism defined (as distinct from 'Cybercrime') - InfoSec resources. Retrieved December 2, 2015, from http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/

INFOSEC. (2013, June 20). Guiding principles in information security - InfoSec resources. Retrieved December 2, 2015, from http://resources.infosecinstitute.com/guiding-principles-in-information-security/

Texas Education Agency. (2015, November 18). Principles of information technology. Retrieved December 1, 2015, from https://cte.unt.edu/information-technology/principles-information-technology

Henderson, A. (2015, July 5). The CIA triad: Confidentiality, integrity, availability - Panmore institute. Retrieved December 2, 2015, from http://panmore.com/the-cia-triad-confidentiality-integrity-availability

Herald, T. K. (2014, July 25). [Weekender] privacy in peril amid prevalence of social media. Retrieved December 1, 2015, from http://www.koreaherald.com/view.php?ud=20140725000866

Jayson, S. (2014, March 12). Social media research raises privacy and ethics issues. . Retrieved from http://www.usatoday.com/story/news/nation/2014/03/08/data-online-behavior-research/5781447/

Green, J. (2006). The myth of cyberterrorism: There are many ways terrorists can kill you—computers aren't one of them. Retrieved December 2, 2015, from http://www.washingtonmonthly.com/features/2001/0211.green.html

Otto, G., (2015, November 18). DHS head: Agency to strike balance between cybersecurity and counterterrorism. Retrieved December 2, 2015, from http://fedscoop.com/dhs-head-agency-looking-to-strike-balance-between-cybersecurity-and-counterterrorism

Singer, P. W., Friedman, A., (2014, January 22). What do we mean by security anyway? Opinions. Retrieved from http://www.brookings.edu/research/opinions/2014/01/22-what-is-security-in-cyberspace-singer-friedman

Air Force Association. AFA CyberPatriot Website. Retrieved December 1, 2015, from http://www.uscyberpatriot.org

Internet Keep Safe Coalition. Cyber Ethics. Retrieved December 1, 2015, from http://ikeepsafe.org/educators_old/more/c3-matrix/cyber-ethics/

Norse. Norse attack map. Retrieved December 2, 2015, from http://map.norsecorp.com/

ISECOM. Security awareness for teens. Retrieved December 2, 2015, from http://www.hackerhighschool.org/

Air Force Association. UNIT FIVE Microsoft windows security. Retrieved December 2, 2015, from https://s3.amazonaws.com/cpvii/Training+materials/Unit+Five+-+Microsoft+Windows+Security.pdf

Recommended course activities:

Lectures, videos, presentations, hands-on labs, operating systems configurations and hardening activities, web exploration and research, and competition simulation

Suggested methods for evaluating student outcomes:

Pre-tests, post-tests, formative and summative assessments, observations, simulations and performance assessment, achievement tests (standardized or non-standardized), peer and self-evaluation, and portfolios

Teacher qualifications:

- ☐ Business and Finance: Grades 6-12
- ☐ Business Education: Grades 6-12
- ☐ Secondary Industrial Arts (Grades 6-12)
- ☐ Secondary Industrial Technology (Grades 6-12)
- ☐ Technology Applications: Grades 8-12
- ☐ Technology Education: Grades 6-12
- ☐ Computer Science (8-12)
- ☐ Secondary Computer Information Systems (Grades 6-12)
- ☐ Trade and Industrial Education: Grades 6-12. This assignment requires appropriate work approval.
- ☐ Vocational Trades and Industry. This assignment requires appropriate work approval.

Approved Innovative Course

- *Districts must have local board approval to implement innovative courses*
- *Innovative courses may meet state elective credit only*
- *CTE Innovative courses may not be the final course in a coherent sequence used for an endorsement*
- *Course requirements must be met without modification*

Additional information: