Information Technology Career Cluster
Advanced Cybersecurity
Course Number : 11.48200

Course Description :
Advanced Cybersecurity is designed to provide students the advanced concepts and terminology of cybersecurity. The course explores the field of cybersecurity with updated content including new innovations in technology and methodologies. It builds on existing concepts introduced in Introduction to Cybersecurity and expands into malware threats, cryptography, organizational security, and wireless technologies.

Various forms of technologies will be used to expose students to resources, software, and applications of cybersecurity. Professional communication skills will be used to expose students to resources, software, and applications of cybersecurity. Professional communication skills and practices, problem-solving, ethical and legal issues, and the impact of effective presentation skills are enhanced in this course to prepare students to be college and career ready. Employability skills are integrated into activities, tasks, and projects throughout the course standards to demonstrate the skills required by business and industry. Competencies in the co-curricular student organization, Future Business Leaders of America (FBLA), are integral components of the employability skills standard for this course.

Advanced Cybersecurity is the third course in the Cybersecurity c832 Tm [(c832 T(e)-6(445.32 Tm [(co)-6(u)

successfully completed Introduction to Digital Technology and Introduction to Cybersecurity.

Course Standard 1

IT-ACS-1
The following standard is included in all CTAE courses adopted for the Career Cluster/Pathways. Teachers should incorporate the elements of this standard into lesson plans during the course. The topics listed for each element of the standard may be addressed in differentiated instruction matching the content of each course. These elements may also be addressed with specific lessons from a variety of resources. This content is not to be treated as a unit or separate body of

		Cell Phone and Internet Etiquette	Communicating At Work	Listening
Interacting with Your Boss	Telephone Conversations	Using Blogs	Improving Communication Skills	Reasons, Benefits, a /MCID 66>> B

1.4 Model work readiness traits required for success in the workplace including integrity, honesty, accountability, punctuality, time management, and respect for diversity.

Workplace Ethics	Personal Characteristics	Employer Expectations	Business Etiquette	Communicating at Work
Demonstrating Good Work Ethic	Demonstrating a Good Attitude	Behaviors Employers Expect	Language and Behavior	Handling Anger
Behaving Appropriately	Gaining and Showing Respect	Objectionable Behaviors	Keeping Information Confidential	Dealing with Difficult Coworkers
Maintaining Honesty	Demonstrating Responsibility	Establishing Credibility	Avoiding Gossip	Dealing with a Difficult Boss
Playing Fair	Showing Dependability	Demonstrating Your Skills	Appropriate Work Email	Dealing with Difficult Customers
Using Ethical Language	Being Courteous	Building Work Relationships	Cell Phone Etiquette	Dealing with Conflict
Showing Responsibility	Gaining		Appropriate Work Texting	

International Etiquette			Demonstrating Leadership
CrossCultural Etiquette			
Working in a Cubicle			

Support of CTAE Foundation Course Standards and Georgia Standards of Excellence L9-10RST 1-10 and L9-10WHST 1-10:
Georgia Standards of Excellence ELA/Literacy standards have been written specifically for technical subjects and have been adopted as part of the official standards for all CTAE courses.

Course Standard 2

IT-ACS-2
Explore concepts of cybersecurity related to legal and ethical decisions .
The following elements should be integrated throughout the content of this course.

2.1 Describe the threats to a computer network, methods of avoiding attacks, and options in dealing with virus attacks.
2.2 Investigate potential abuse and unethical uses of computers and networks.
2.3 Explain the consequences of illegal, social, and unethical uses of information technologies (e.g., piracy; illegal downloading; licensing infringement; inappropriate uses of software, hardware, and mobile devices).
2.4 Differentiate between freeware, shareware, and public domain software copyrights.
2.5 Discuss computer crimes, terms of use, and legal issues such as copyright laws, fair use laws, and ethics pertaining to scanned and downloaded clip art images, photographs, documents, video, recorded sounds and music, trademarks, and other elements for use in Web publications.
2.6 Identify netiquette including the use of e-mail, social networking, blogs, texting, and chatting.
2.7 Explain proper netiquette, including the use of e-mail, social networking, blogs, texting, and chatting.
2.8 Discuss the importance of cyber safety and the impact of cyber bullying.

Course Standard 3

IT-ACS-3
Investigate concepts of malware threats .

3.1 Analyze and differentiate among types of malware.
3.2 Identify malware code, including strings.
3.3 Demonstrate skill in handling malware. [NICE 153]
3.4 Demonstrate skill in preserving evidence integrity according to standard operating procedures or national standards. [NICE 217].

Course Standard 4

IT-ACS-4
Demonstrate how to analyze and react to various threats and vulnerabilities.

4.1 Analyze and differentiate among types of network attacks (e.g., virus, worms, trojans, unpatched software, password cracking, advanced persistent threats, etc.).
4.2 Distinguish between different social engineering attacks (e.g., baiting, phishing/spear phishing, pretexting/ blagging, tailgating, quid pro quo, etc.).
4.3 Distinguish between reconnaissance/footprinting, infiltration, network breach, network exploitation, and attack for effects (e.g., deceive, disrupt, degrade, and destroy).

8.5 Perform imaging functions, such as operating system, network, and software configurations.
8.6 Restore a machine from a known good backup.

Course Standard 9

IT-ACS-9
Perform security analysis, as well as testing and evaluation.

9.1 Analyze and differentiate among types of mitigation and deterrent techniques.
9.2 Implement assessment tools and techniques to discover security threats and vulnerabilities.
9.3 Explain the proper use of penetration testing versus vulnerability scanning in the context of vulnerability assessments.
9.4 Demonstrate skill in conducting vulnerability scans and recognizing vulnerabilities in security systems (e.g., Nessus, Nmap, Retina). [NICE 3]
9.5 Conduct a security audit.
9.6 View and modify an Address Resolution Protocol (ARP) table.
9.7 Evaluate the patch status of a machine.
9.8 Demonstrate knowledge of packet-level analysis in order to install and view packet sniffer. [NICE 93]
9.9 Perform secure data destruction (e.g., Secure Erase, BCWipe).

Course Standard 10

IT-ACS-10
Implement risk management techniques for personal computer and network systems.

10.1 Explain risk-related concepts.
10.2 Perform a risk assessment.
10.3 Identify mitigations for risks from risk assessment.
10.4 Conduct appropriate risk mitigation strategies.

Course Standard 11

IT-ACS-11
Demonstrate how to work with advanced methods of cybersecurity.

11.1 Apply and implement secure network administration principles.
11.2 Demonstrate knowledge of how network services and protocols interact to provide network communications in order to securely implement and use common protocols. [NICE 50]
11.3 Identify commonly used default network ports.
11.4 Set up a Network Address Translation (NAT) device.
11.5 Spoof a Media Access Control (MAC) address.
11.6 Configure Virtual Private Network (VPN).
11.7 Configure remote access policy. [illegible]

11.10 Demonstrate the knowledge and use of network statistics (netstat), a command purpose.

Course Standard 12

IT-ACS-12
Explore how related student organizations are integral parts of career and technology education courses through leadership development, school and community service projects, entrepreneurship development, and competitive events.

12.1 Explain the goals, mission and objectives of Future Business Leaders of America.
12.2 Explore the impact and opportunities a student organization (FBLA) can develop to bring business and education together in a positive working relationship through innovative leadership and career development programs.
12.3 Explore the local, state, and national opportunities available to students through participation in related student organization (FBLA) including but not limited to conferences, competitions, community service, philanthropy, and other FBLA activities.
12.4 Explain how participation in career and technology education student organizations can promote lifelong responsibility for community service and professional development.
12.5 Explore the competitive events related to the content of this course and the required competencies, skills, and knowledge for each related event for individual, team, and chapter competitions.