Georgia CTAE

Advanced Cyber Security (11.48200) (2014)

Adopted 2014

Demonstrate employability skills required by business and industry. IT-ACS-1

1. **Communicate effectively through writing, speaking, listening, reading, and interpersonal abilities.** IT-ACS-1.1
2. **Demonstrate creativity by asking challenging questions and applying innovative procedures and methods.** IT-ACS-1.2
3. **Exhibit critical thinking and problem solving skills to locate, analyze and apply information in career planning and employment situations.** IT-ACS-1.3
4. **Model work readiness traits required for success in the workplace including integrity, honesty, accountability, punctuality, time management, and respect for diversity.** IT-ACS-1.4
5. **Apply the appropriate skill sets to be productive in a changing, technological, diverse workplace to be able to work independently and apply team work skills.** IT-ACS-1.5
6. **Present a professional image through appearance, behavior and language.** IT-ACS-1.6

Explore concepts of cybersecurity related to legal and ethical decisions. IT-ACS-2

1. **Describe the threats to a computer network, methods of avoiding attacks, and options in dealing with virus attacks.** IT-ACS-2.1
2. **Investigate potential abuse and unethical uses of computers and networks.** IT-ACS-2.2
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).** IT-ACS-2.3
4. **Differentiate between freeware, shareware, and public domain software copyrights.** IT-ACS-2.4
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.** IT-ACS-2.5

	6. Identify netiquette including the use of e-mail, social networking, blogs, texting, and chatting. IT-ACS-2.6
	7. Explain proper netiquette, including the use of e-mail, social networking, blogs, texting, and chatting. IT-ACS-2.7
	8. Discuss the importance of cyber safety and the impact of cyber bullying. IT-ACS-2.8
Investigate concepts of malware threats. IT-ACS-3	1. Analyze and differentiate among types of malware. IT-ACS-3.1
	2. Identify malware code, including strings. IT-ACS-3.2
	3. Demonstrate skill in handling malware. IT-ACS-3.3
	4. Demonstrate skill in preserving evidence integrity according to standard operating procedures or national standards. IT-ACS-3.4
Demonstrate how to analyze and react to various threats and vulnerabilities. IT-ACS-4	1. Analyze and differentiate among types of network attacks (e.g., virus, worms, trojans, unpatched software, password cracking, advanced persistent threats, etc.). IT-ACS-4.1
	2. Distinguish between different social engineering attacks (e.g., baiting, phishing/spear phishing, pretexting/ blagging, tailgating, quid pro quo, etc.). IT-ACS-4.2
	3. Distinguish between reconnaissance/footprinting, infiltration, network breach, network exploitation, and attack for effects (e.g., deceive, disrupt, degrade, and destroy). IT-ACS-4.3
	4. Demonstrate an understanding of DoS/DDoS, session hijacking, HTTP spoofing, DNS attacks, switch attacks, man-in-the-middle (MITM) attacks, and cross site scripting, and drive-by-attacks. IT-ACS-4.4
Apply advanced principles of cryptology. IT-ACS-5	1. Use and apply appropriate cryptographic tools and products. IT-ACS-5.1
	2. Explain the core concepts of Public Key Infrastructure. IT-ACS-5.2
	3. Demonstrate knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]) and implement PKI, certificate management, and associated components. IT-ACS-5.3
	4. Install and configure Pretty Good Privacy (PGP) and send/receive PGP encrypted email. IT-ACS-5.4
	5. Install and view a digital certificate. IT-ACS-5.5
	6. Understand and master process to enroll for digital certificates. IT-ACS-5.6

	7. **Renew, revoke, backup, and restore public and private key certificates.** IT-ACS-5.7
	8. **Install and secure a Certificate Authority (CA).** IT-ACS-5.8
	9. **Backup and restore a Certificate Authority (CA).** IT-ACS-5.9
Apply advanced communications and wireless security techniques. IT-ACS-6	1. **Implement wireless networks in a secure manner.** IT-ACS-6.1
	2. **Analyze and differentiate among types of wireless attacks.** IT-ACS-6.2
	3. **Configure a wireless Access Point (WPA, WPA-2).** IT-ACS-6.3
	4. **Demonstrate use of InSSIDer and Netstumbler on wireless communications.** IT-ACS-6.4
	5. **Change the power level of a Wireless Local Area Network (WLAN) Access Point.** IT-ACS-6.5
	6. **Demonstrate knowledge of Virtual Private Network (VPN) security and configure Virtual Private Network (VPN).** IT-ACS-6.6
	7. **Demonstrate knowledge of remote access policy Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP).** IT-ACS-6.7
Implement organizational security techniques. IT-ACS-7	1. **Explain the impact and proper use of environmental controls.** IT-ACS-7.1
	2. **Explain the importance of security-related awareness and training.** IT-ACS-7.2
	3. **Install environmental controls through Basic Input/Output System (BIOS).** IT-ACS-7.3
	4. **Write organizational security policies (email, wireless, etc.).** IT-ACS-7.4
Implement contingency planning (incident response and disaster recovery) techniques. IT-ACS-8	1. **Demonstrate knowledge of incident response and handling methodologies.** IT-ACS-8.1
	2. **Demonstrate knowledge of incident categories, incident responses, and timelines for responses and compare and contrast aspects of business continuity.** IT-ACS-8.2
	3. **Execute disaster recovery plans and procedures.** IT-ACS-8.3
	4. **Demonstrate the ability to capture volatile memory contents.** IT-ACS-8.4
	5. **Perform imaging functions, such as operating system, network, and software configurations.** IT-ACS-8.5
	6. **Restore a machine from a known good backup.** IT-ACS-8.6

Perform security analysis, as well as testing and evaluation. IT-ACS-9	1. **Analyze and differentiate among types of mitigation and deterrent techniques.** IT-ACS-9.1 2. **Implement assessment tools and techniques to discover security threats and vulnerabilities.** IT-ACS-9.2 3. **Explain the proper use of penetration testing versus vulnerability scanning in the context of vulnerability assessments.** IT-ACS-9.3 4. **Demonstrate skill in conducting vulnerability scans and recognizing vulnerabilities in security systems (e.g., Nessus, Nmap, Retina).** IT-ACS-9.4 5. **Conduct a security audit.** IT-ACS-9.5 6. **View and modify an Address Resolution Protocol (ARP) table.** IT-ACS-9.6 7. **Evaluate the patch status of a machine.** IT-ACS-9.7 8. **Demonstrate knowledge of packet-level analysis in order to install and view packet sniffer.** IT-ACS-9.8 9. **Perform secure data destruction (e.g., Secure Erase, BCWipe).** IT-ACS-9.9
Implement risk management techniques for personal computer and network systems. IT-ACS-10	1. **Explain risk-related concepts.** IT-ACS-10.1 2. **Perform a risk assessment.** IT-ACS-10.2 3. **Identify mitigations for risks from risk assessment.** IT-ACS-10.3 4. **Conduct appropriate risk mitigation strategies.** IT-ACS-10.4
Demonstrate how to work with advanced methods of cybersecurity. IT-ACS-11	1. **Apply and implement secure network administration principles.** IT-ACS-11.1 2. **Demonstrate knowledge of how network services and protocols interact to provide network communications in order to securely implement and use common protocols.** IT-ACS-11.2 3. **Identify commonly used default network ports.** IT-ACS-11.3 4. **Set up a Network Address Translation (NAT) device.** IT-ACS-11.4 5. **Spoof a Media Access Control (MAC) address.** IT-ACS-11.5 6. **Configure Virtual Private Network (VPN).** IT-ACS-11.6 7. **Configure a remote access policy Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP).** IT-ACS-11.7

8. **Demonstrate knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol (TCP/IP), Dynamic Host Configuration Protocol (DHCP) and directory services (e.g., Domain Name System (DNS) by setting up common protocols, e.g., Secure Shell (SSH), netstat, Simple Mail Transfer Protocol (SMTP), nslookup, Telnet, DNS/Bind, FTP, IIS/Web Pages, DHCP/DNS server.** IT-ACS-11.8
9. **Locate open ports by completing a port scan.** IT-ACS-11.9
10. **Demonstrate the knowledge and use of network statistics (netstat), a command purpose.** IT-ACS-11.10

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. IT-ACS-12

1. **Explain the goals, mission and objectives of Future Business Leaders of America.** IT-ACS-12.1
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.** IT-ACS-12.2
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.** IT-ACS-12.3
4. **Explain how participation in career and technology education student organizations can promote lifelong responsibility for community service and professional development.** IT-ACS-12.4
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.** IT-ACS-12.5