ADVANCED CYBER SECURITY
COURSE CODE: 5372

COURSE DESCRIPTION: In Advanced Cyber Security, the second course in the Computer and Information Systems Security/Information Assurance program, students will examine the advanced concepts and terminology of cyber security and information assurance, secure systems and networks against threats, attacks, and vulnerabilities by implementing appropriate architecture and design, implementation of security protocols and controls, operations and incident responses, governance, risk management and compliance. Upon completion of the two courses, students will be prepared to earn industry professional certification(s).

OBJECTIVE: Given the necessary equipment, supplies, and appropriate software, the student will be prepared to successfully complete the standards necessary for national credentials.

COURSE CREDIT: 1 (120 hours) or 2 (240 hours) units

PREREQUISITE: Cyber Security Fundamentals

RECOMMENDED GRADE LEVEL: 10 – 12

RESOURCES: Instructional Materials

A. SAFETY

Proficient professionals know the academic subject matter, including safety as required for proficiency within their area. They will use this knowledge as needed in their role. The following accountability criteria are considered essential for students in any program of study.

1. Review school safety policies and procedures.
2. Review classroom safety rules and procedures.
3. Review safety procedures for using equipment in the classroom.
4. Identify major causes of work-related accidents in office environments.
5. Demonstrate safety skills in an office/work environment.

B. STUDENT ORGANIZATIONS

Proficient professionals know the academic subject matter, including professional development. They will use this knowledge as needed in their role. The following accountability criteria are considered essential for students in any program of study.

1. Identify the purpose and goals of a Career and Technology Student Organization (CTSO).
2. Explain how CTSOs are integral parts of specific clusters, majors, and/or courses.
3. Explain the benefits and responsibilities of being a member of a CTSO.
4. List leadership opportunities that are available to students through participation in CTSO conferences, competitions, community service, philanthropy, and other activities.
5. Explain how participation in CTSOs can promote lifelong benefits in other professional and

civic organizations.

B. TECHNOLOGY KNOWLEDGE

Proficient professionals know the academic subject matter, including the ethical use of technology. The following accountability criteria are considered essential for students in any program of study.

1. Demonstrate proficiency and skills associated with the use of technologies that are common to a specific occupation.
2. Identify proper netiquette when using e-mail, social media, and other technologies for communication purposes.
3. Identify potential abuse and unethical uses of laptops, tablets, computers, and/or networks.
4. Explain the consequences of social, illegal, and unethical uses of technology (e.g., piracy; cyberbullying, illegal downloading; licensing infringement; inappropriate uses of software, hardware, and mobile devices in the work environment).
5. Discuss legal issues and the terms of use related to copyright laws, fair use laws, Creative Commons, and ethics pertaining to downloading of images, photographs, documents, video, sounds, music, trademarks, and other elements for personal use.
6. Describe ethical and legal practices of safeguarding the confidentiality of business-related information.
7. Describe possible threats to a laptop, tablet, computer, and/or network and methods of avoiding attacks.

C. PERSONAL QUALITIES AND EMPLOYABILITY SKILLS

Proficient professionals know the academic subject matter, including positive work practices and interpersonal skills. The following accountability criteria are considered essential for students in any program of study.

1. Demonstrate creativity and innovation.
2. Demonstrate critical thinking and problem-solving skills.
3. Demonstrate initiative and self-direction.
4. Demonstrate integrity.
5. Demonstrate work ethic.
6. Demonstrate conflict resolution skills.
7. Demonstrate listening and speaking skills.
8. Demonstrate respect for diversity.
9. Demonstrate customer service orientation.
10. Demonstrate teamwork.

E. PROFESSIONAL KNOWLEDGE

Proficient professionals know the academic subject matter, including positive work practices and interpersonal skills. The following accountability criteria are considered essential for students in any program of study.

1. Demonstrate global or “big picture” thinking.

2. Demonstrate career and life management skills and goal-making.
3. Demonstrate continuous learning and adaptability skills to changing job requirements.
4. Demonstrate time and resource management skills.
5. Demonstrates information literacy skills.
6. Demonstrates information security skills.
7. Demonstrates information technology skills.
8. Demonstrates knowledge and use of job-specific tools and technologies.
9. Demonstrate job-specific mathematics skills.
10. Demonstrates professionalism in the workplace.
11. Demonstrate reading and writing skills.
12. Demonstrates workplace safety.

DOMAINS SUPPORTING COMPTIA SECURITY + CERTIFICATION

F. THREATS, ATTACKS, AND VULNERABILITIES

Proficient IT professionals demonstrate knowledge of cyber threats, attacks, and vulnerabilities. The following accountability criteria are considered essential for students in the Computer and Information Systems Security/Information Assurance program of study.

1. Compare and contrast different types of social engineering techniques (e.g., Phishing, Spam, Spear phishing, Identity fraud).
2. Given a scenario, analyze potential indicators to determine the type of attack (e.g., Malware, Password attacks, Physical attacks, Cryptographic attacks).
3. Given a scenario, analyze potential indicators associated with application attacks (e.g., Error handling, Race conditions, Integer overflow, Memory leaks).
4. Given a scenario, analyze potential indicators associated with network attacks (e.g., Wireless, On-path attack, Domain Name System (DNS), Malicious code).
5. Explain different threat actors, vectors, and intelligence sources (e.g., Actors and threats, Vectors, Attributes of actors).
6. Explain the security concerns associated with various types of vulnerabilities (e.g., Third-party risks, Weak configurations, Zero-day, Legacy platform).
7. Summarize the techniques used in security assessments (e.g.,Threat hunting, Vulnerability scans, Syslog/Security information) .
8. Explain the techniques used in penetration testing (e.g., Penetration testing, Passive and active reconnaissance, Exercise Types).

G. ARCHITECTURE AND DESIGN

Proficient IT professionals demonstrate knowledge of security architecture and design. The following accountability criteria are considered essential for students in the Computer and Information Systems Security/Information Assurance program of study.

1. Explain the importance of security concepts in an enterprise environment (e.g., Configuration management, Data protection, Hashing, Site resiliency).
2. Summarize virtualization and cloud computing concepts (e.g., Cloud models, Cloud service providers, Containers, Microservices/API).

3. Summarize secure application development, deployment, and automation concepts (e.g., Environment, Secure coding techniques, Scalability, Automation/scripting).
4. Summarize authentication and authorization design concepts (e.g., Biometrics, Multifactor authentication, Cloud vs on-premises requirements).
5. Given a scenario, implement cybersecurity resilience (e.g., Redundancy, Network, Power, Replication, Diversity).
6. Explain the security implications of embedded and specialized systems (e.g., Voice over IP(VoIP), System on Chip (SoC), Constraints, Surveillance systems).
7. Explain the importance of physical security controls (e.g., Badges, Alarms, Cameras, Locks, Secure Areas).
8. Summarize the basics of cryptographic concepts (e.g., Digital signatures, Key length, Symmetric vs asymmetric, Limitations).

H. IMPLEMENTATION

Proficient IT professionals demonstrate knowledge of implementation standards. The following accountability criteria are considered essential for students in the Computer and Information Systems Security/Information Assurance program of study.

1. Given a scenario, implement secure protocols (e.g., Protocols, Use cases).
2. Given a scenario, implement host or application security solutions (e.g., Endpoint protection, Boot integrity, BIOS, Database, Application security, Hardening, Self-encrypting drive (SED), Full-disk encryption (FDE), Hardware root of trust, Trusted Platform Module (TPM), sandboxing).
3. Given a scenario, implement secure network designs (e.g., Load balancing, Network segmentation, virtual private network (VPN), DNS, network access control (NAC), Out-of-band management, port security, network appliances, Access control list (ACL), route security, Quality of service (QoS), implications of IPv6, Port spanning/port mirroring, monitoring services, file integrity monitors).
4. Given a scenario, install and configure wireless security settings (e.g., Cryptographic protocols, Authentication protocols, Methods, Installation considerations).
5. Given a scenario, implement secure mobile solutions (e.g., connection methods and receivers, Mobile Device Management (MDM), mobile devices, enforcement and monitoring, deployment models).
6. Given a scenario, implement secure mobile solutions (e.g., cloud security controls, solutions, cloud native controls vs. third-party solutions).
7. Given a scenario, implement identity and account management controls (e.g., identity, account types, account policies).
8. Given a scenario, implement authentication and authorization solutions (e.g., Authentication management, authentication/authorization, access control schemes).
9. Given a scenario, implement public key infrastructure (e.g., Public Key Infrastructure (PKI), types of certificates, certificate formats, concepts).

I. OPERATIONS AND INCIDENT RESPONSE

Proficient IT professionals demonstrate knowledge of operations and incident response. The following accountability criteria are considered essential for students in the Computer and Information Systems Security/Information Assurance program of study.

1. Given a scenario, use the appropriate tool to assess organizational security (e.g., forensics, file manipulation, network reconnaissance and discovery, password crackers).
2. Summarize the importance of policies, processes, and procedures for incident response (e.g., incident response plans and process, exercises, attack frameworks, communication plan).
3. Given an incident, utilize appropriate data sources to support an investigation (e.g., log files, protocol analyzer output, bandwidth monitors, metadata).
4. Given an incident, apply mitigation techniques or controls to secure an environment (e.g., configuration changes, isolation, containment, segmentation).
5. Explain the key aspects of digital forensics (e.g., documentation/evidence, acquisition, Integrity, data recovery, preservation).
6. Perform secure data destruction (e.g., Secure Erase, BCWipe).

J. GOVERNANCE, RISK, AND COMPLIANCE

Proficient IT professionals demonstrate knowledge of governance, risk, and compliance. The following accountability criteria are considered essential for students in the Computer and Information Systems Security/Information Assurance program of study.

1. Compare and contrast various types of controls (e.g., managerial, preventative, corrective, deterrent).
2. Explain the importance of applicable regulation standards or frameworks that impact organization security posture (e.g., General Data Protection Regulation (GDPR), - Center for Internet Security (CIS), International Organization for Standardization (ISO) 27001/27002/27701/31000, platform/vendor-specific guides).
3. Explain the importance of policies to organizational security (e.g., personnel, diversity of training techniques, third-party risk management, data, credential policies, organizational policies).
4. Summarize risk management processes and concepts (e.g., risk types, risk management strategies, risk analysis, disasters, business impact analysis).
5. Explain privacy and sensitive data concepts in relation to security (e.g., organizational consequences of privacy and data breaches, notifications of breaches, data types, privacy enhancing technologies, roles and responsibilities).

Additional Materials and Resources

Academic Standards and Indicators

Computer Science Academic Alignment