CYBER SECURITY FUNDAMENTALS
COURSE CODE: 5370
STUDENT PROFILE

STUDENT'S NAME:	**TEACHER'S NAME:**
School Year/Semester:	**Grade:**
Begin Date:	**Date Completed:**

Directions: Document student's progress using the applicable rating scales below: Enter date of completion under the appropriate column.

0 - Requires additional instruction and or **close supervision (60-69)**
1 – Has not received instruction in this area / **no experience or knowledge of this task (N/A)**
2 – Can perform the task completely with **limited supervision (70-79)**
3 – Can apply and perform **independently (80-100)**

A. SAFETY		**0**	**1**	**2**	**3**
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		**0**	**1**	**2**	**3**
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.				
C. TECHNOLOGY KNOWLEDGE		**0**	**1**	**2**	**3**
1	Demonstrate proficiency and skills associated with the use of technologies that are common to a specific occupation (e.g., keying speed).				
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., cyber bullying; piracy; illegal downloading; cyberbullying; 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, and ethics pertaining to downloading of images, photographs, Creative Commons, 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.				
8	Evaluate various solutions to common hardware and software problems.				
D. PERSONAL QUALITIES AND EMPLOYABILITY SKILLS		**0**	**1**	**2**	**3**
1	Demonstrate punctuality.				
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		**0**	**1**	**2**	**3**
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	Demonstrates reading and writing skills.				
12	Demonstrates workplace safety.				
F. INTRODUCTION TO CYBER SECURITY		**0**	**1**	**2**	**3**
1	Define terms related to cyber security (e.g., cyber security, information assurance, risk, risk management, cyber security services).				
2	Explain the importance of information and internet security (e.g., browser, cloud, network).				
3	Explain the concepts of confidentiality, integrity, and availability (CIA).				
4	Identify the concepts of cyber security risk management. (e.g., vulnerability identification, management, and mitigation; active and passive reconnaissance; testing port scanning, automation).				
5	Explain vulnerability management (e.g., identification, management, mitigation, testing).				
6	Describe cyber security threats to an organization and why organizations need to manage risk.				
7	Research potential consequences of various forms of security incidents.				
8	Compare and contrast the various types of security (e.g., physical security, technological, administrative).				
9	Research national or industry standards/regulations that relate to cyber security and their impact on people, processes, and technology (e.g., news, reports, policies, subscriptions, incidents).				
10	Investigate the origins and history of cyber security and its impact on society.				
11	Describe the role that cyber security plays in the private or public sector.				
12	Discuss and develop a code of ethics as related to the field of cyber security.				

G. CYBER THREATS AND VULNERABILITIES		0	1	2	3
1	Describe the characteristics of cyber threats, attacks, and vulnerabilities.				
2	Analyze types of current cyber threats (e.g., DDoS, Phishing, cracking, social engineering).				
3	Categorize sources/originators of different types of malicious attacks (e.g., nation states, cyber criminals, hacktivists, insiders).				
4	Compare and contrast cyber-attack surfaces of differing organizations.				
5	Explain types of malware (e.g., viruses, polymorphic viruses; worms, Trojan horses, spyware, ransomware, adware).				
6	Demonstrate familiarity with malware removal (e.g. scanning systems, reviewing scan logs, malware remediation).				
7	Explain types of attacks (e.g., wireless, application, social engineering, buffer overflow attacks, backdoor).				
8	Define strategies necessary to prevent attacks.				
H. COMPUTER AND NETWORK ARCHITECTURE		**0**	**1**	**2**	**3**
1	Define terms related to computer networking (e.g., LAN, WAN, wireless, protocols, topology, firewalls).				
2	Compare and contrast OSI and TCP/IP models and encapsulation concepts.				
3	Compare and contrast wired versus wireless networks.				
4	Examine the concept of the internet as a network of connected systems.				
5	Design a basic network topology.				
I. NETWORK SECURITY		**0**	**1**	**2**	**3**
1	Define terms related to network security (e.g., routing, perimeter networks, security layering, Virtual Private Network (VPN), isolation).				
2	Explain the concepts of protocol security (e.g., protocol spoofing, tunneling, network sniffing, denial of service).				
3	Analyze and implement security layering.				
4	Identify vulnerabilities and common attack methods.				
5	Use strategies necessary to prevent network attacks.				
6	Identify tools and techniques used for security layering.				
7	Determine characteristics of firewalls (hardware and software) and when to use them.				
8	Set up Port/Network Address Translation (NAT/PAT).				
9	Explain how network addresses impact network security (e.g., IPv4 and IPv6 addressing, CIDR notation, public vs private networks.				

10	Use a basic command line interface (Windows and Linux) to configure communications (e.g., ipconfig, ifconfig, and net config, ping).				
J. OPERATING SYSTEMS		**0**	**1**	**2**	**3**
1	Compare and contrast common operating systems (e.g., Windows, Linux, iOS, Android).				
2	Identify best practices for protecting operating systems (e.g., access control, separation of duties, least privilege).				
3	Compare and contrast common file systems (e.g., FAT, NTFS, HFS).				
4	Describe the various types of file permissions (e.g., registry, Active Directory, basic and advanced).				
5	Implement group and audit policies.				
6	Explain the purpose and location of security and auditing logs.				
7	Define virtualization and identify its advantages and disadvantages.				
8	Define strategies necessary to prevent operating system attacks.				
K. OPERATIONAL SECURITY		**0**	**1**	**2**	**3**
1	Define terms related to identity, authorization, and authentication (e.g., passwords, biometrics, multi-factor, certificates).				
2	Describe the various types of permissions (e.g., basic, administrative, elevated).				
3	Identify types of access control (e.g., role-based access control (RBAC), mandatory access control, discretionary-based control).				
4	Describe the importance of Multifactor authentication.				
5	Analyze best practices for end-user password development and usage.				
6	Identify the system administrator’s role in setting system policies and procedures.				
7	Compare and contrast backup and restore methods.				
8	Explain the importance of disaster recovery and business continuity planning (e.g., disaster recovery plans and controls, business continuity plans, backups).				
9	Secure servers (e.g., DNS/BIND, web, email, messaging, FTP, directory services, DHCP, file and print servers).				
L. CRYPTOGRAPHY		**0**	**1**	**2**	**3**
1	Define cryptography and its related terms (e.g., encryption, decryption, public key, and private key).				
2	Identify encryption methods (e.g., symmetric and asymmetric).				
3	Determine appropriate uses for encrypting data and connections (e.g., email, files, network, VPN).				

4	Explain how the design and functionality of various encryption methods support the security of data.				
5	Demonstrate various encryption techniques (e.g., encryption algorithms, Encrypting File System (EFS), hashing, public and private keys, Public Key Infrastructure (PKI), token devices, Trusted Platform Module (TPM), Transport Layer Security (TLS).				
M. SYSTEM SECURITY		**0**	**1**	**2**	**3**
1	Analyze and differentiate between types of system attacks (e.g., operating systems, files, and applications).				
2	Implement security patches and updates (e.g., Active X, Java).				
3	Implement strategies necessary to prevent attacks (e.g., buffer overflow, application, input validation, scripting).				
N. INCIDENT HANDLING		**0**	**1**	**2**	**3**
1	Monitor security events and know when escalation is required (e.g., role of SIEM and SOAR, packet captures, log file entries, identifying suspicious events).				
2	Explain digital forensics and attack attribution processes (cyber kill chain, sources of evidence, evidence handling).				
3	Explain the impact of compliance frameworks on incident handling (e.g., compliance frameworks (GDPR, HIPAA, PCI-DSS, FERPA, FISMA), reporting and notification requirements).				
4	Describe the elements of cybersecurity incident response (e.g., policy plan procedure elements, incident response lifecycle stages).				