

# Cybersecurity I

<b>Primary Career Cluster:</b>	Information Technology
<b>Consultant:</b>	Deborah Knoll, (615) 532-2844, <a href="mailto:Deborah.Knoll@tn.gov">Deborah.Knoll@tn.gov</a>
<b>Course Code(s):</b>	
<b>Prerequisite(s):</b>	<i>Algebra I</i> (0842, 3102), <i>Computer Science Foundations</i> (6095)
<b>Credit:</b>	1
<b>Grade Level:</b>	10
<b>Graduation Requirements:</b>	This course satisfies one of three credits required for an elective focus when taken in conjunction with other Information Technology courses.
<b>Programs of Study and Sequence:</b>	This is the second course in the <i>Cybersecurity</i> program of study.
<b>Aligned Student Organization(s):</b>	SkillsUSA: <a href="http://www.tnskillsusa.com">http://www.tnskillsusa.com</a> Tracy Whitehead, (615) 532-2804, <a href="mailto:Tracy.Whitehead@tn.gov">Tracy.Whitehead@tn.gov</a> Technology Student Association (TSA): <a href="http://www.tntsa.org">http://www.tntsa.org</a> Tracy Whitehead, (615) 532-2804, <a href="mailto:Tracy.Whitehead@tn.gov">Tracy.Whitehead@tn.gov</a>
<b>Coordinating Work-Based Learning:</b>	Teachers are encouraged to use embedded WBL activities such as informational interviewing, job shadowing, and career mentoring. For information, visit <a href="https://tn.gov/education/topic/work-based-learning">https://tn.gov/education/topic/work-based-learning</a> .
<b>Available Student Industry Certifications:</b>	None
<b>Dual Credit or Dual Enrollment Opportunities:</b>	There are no statewide dual credit/dual enrollment opportunities for this course. If interested in establishing a local opportunity, reach out to a local postsecondary institution.
<b>Teacher Endorsement(s):</b>	
<b>Required Teacher Certifications/Training:</b>	
<b>Teacher Resources:</b>	<a href="https://tn.gov/education/article/cte-cluster-information-technology">https://tn.gov/education/article/cte-cluster-information-technology</a>

## Course Description

*Cybersecurity I* is a course intended to teach students the basic concepts of cybersecurity. The course places an emphasis on security integration, application of cybersecurity practices and devices, ethics, and best practices management. The fundamental skills in this course cover both in house and external threats to network security and design, how to enforce network level security policies, and how to safeguard an organization's information. Upon completion of this course, proficient students will be demonstrate and understanding of cybersecurity concepts, identify fundamental principles of networking systems, understand network infrastructure and network security, and be able to demonstrate how to implement various aspects of security within a networking system.

## Program of Study Application

This program offers a sequence of courses that provides coherent and rigorous content aligned with challenging academic standards and relevant technical knowledge and skills needed to prepare for further education and

cybersecurity-related careers in the Information Technology career cluster. This is the second course in the *Cybersecurity* program of study. For more information on the benefits and requirements of implementing this program in full, please visit the Information Technology website at <https://tn.gov/education/article/cte-cluster-information-technology>.

## **Course Standards**

### **Cybersecurity Fundamental Concepts**

- 1) Using websites and journals from professional organizations related to information technology, analyze ethical security practices, including but not limited to the issues of data security, confidentiality, integrity, availability, authentication, nonrepudiation, physical security, HIPPA Laws, Payment Card Industry (PCI) Compliance, and the importance of ISO27000 standards.
- 2) Using news articles, research current events on breaches; focus on particular Information Assurance (IA) areas that were compromised. For example, research and report on the effects of unethical security breaches on a business citing specific textual evidence.
- 3) Consult a variety of sources to analyze security threats, vulnerabilities, and exploits. Research common ways that threats, vulnerabilities, and exploits impact an organization. For example, research and report on the threats, vulnerabilities, and exploit(s) used in a recent high profile breach.

### **Risk Management Techniques**

- 4) Read and interpret technical information to define risk management and how it applies to information security. Examine a case study of a company using a systematic approach for the identification, assessment and management of information security risks and compile a brief narrative summarizing conclusions.
- 5) Perform a simulated risk assessment by using the common industry framework from ISO. Analyze and describe the risk mitigation techniques of acceptance, mitigation, avoidance, and transfer.

### **Access Controls**

- 6) Gather relevant information from textbooks and online resources to explain the core concepts of access control as they relate to authentication and authorization. Create an infographic a security analyst could use as a guide.
- 7) Interpret instructional materials to analyze and describe the core principles of access controls. Instructional material may include textbooks, manuals, websites, video tutorials, and more. For example, analyze the use of administrative, logical (technical) and physical controls applied to systems, and organizations.
- 8) Demonstrate the use of access controls that apply to user account management, including basic and advanced techniques. Drawing on evidence from textbooks and other resources, evaluate the effectiveness of the controls and incorporate feedback when refining techniques.

### **Fundamental Principles of Networking**



- 9) Prepare informational artifacts (e.g., brochure, poster, fact sheet, narrative, or presentation) for the following LAN topics:
  - a. Identify and describe common LAN methodologies
  - b. Analyze the various LAN topologies including perimeter networks which may include the use of a DMZ.
  - c. Indicate and explain the standards of Ethernet.
  - d. Describe the characteristics of LAN cabling.
- 10) Explain the industry standards used in wireless networks including security protocols used to protect the wireless network. Read and interpret trade journals, assessing the usefulness of each source, to describe the impact the protocol has had on a particular network. For example, cite evidence from trade journals to explain the Secure Socket Layer (SSL) and Transport Layer Security (TLS) Protocols and their impact on the security of wireless networks.
- 11) Consult a variety of sources to describe how routing protocols are used and the differences between static and dynamic methods of routing. Sources may include textbooks, manuals, websites, video tutorials, and more. Create a visual display with accompanying text comparing and contrasting these two methods.
- 12) Create an illustrative guide that explains how to install and configure Routing and Remote Access Service (RRAS) to function as a network router and how to install and configure Routing Information Protocols.
- 13) Choose between technologies and topologies utilized for WAN networks and justify the choices. Make a written case for selecting one technology and topologies over another, highlighting the features of each and citing resources to validate claims.
- 14) Explain how the different types of personal and small business internet connectivity has changed throughout history, and identify current internet systems most commonly used. Consult internet forums, textbooks, industry journals and other instructional materials, assessing the usefulness of each source, to describe the impact these changes have made. Create and present a document and/or illustration depicting the timeline of development that led to modern-day internet systems citing specific textual evidence.

#### **Fundamental Principles of Open Systems and Internet Protocol**

- 15) Identify, describe, and effectively summarize the common OSI model and the functions used by each layer. Create a written report or visual depiction outlining the characteristics and properties of each.
- 16) Research and create an informational artifact (e.g., brochure, poster, fact sheet, narrative, or presentation) analyzing and describing the differences between the TCP/IP and OSI models for networking.
- 17) Define and describe the various services used by networks for the transmission of data such as DNS, NAT, and DHCP. Create a graphic illustration showing the roles of each service and describe their differences.
- 18) Analyze the differences among the addressing techniques used by networks, including IPv4 and basic IPv6. Write a brief paper that discusses the differences. Provide specific examples to support the claims.

- 19) Using instructional materials, analyze then demonstrate the use of subnets in an organizations network environment. For example, create a simple network using subnets for different organizational locations. Instructional materials may include textbooks, instructional manuals, websites, video tutorials, and more.
- 20) Research the features and requirements of a working model of a client server network and how services function in a networked windows environment. Drawing on multiple resources, demonstrate installation of the various network services in the client server network.

### **Network Infrastructures and Network Security**

- 21) Compare and contrast the differences and uses of the Internet, Intranets, and Extranets. Citing specific examples, create an illustrative guide that outlines the benefits of each and major similarities and differences.
- 22) Research and describe the most common various methods and technology used to secure networks. Investigate and distinguish among the following common methods to secure a network.
  - a. VPNs for remote access
  - b. Firewalls
  - c. Perimeter network designs
  - d. Preventative technologies

### **Fundamental Network Components of Cybersecurity**

- 23) Research the different applications of network security devices. Create a table or other graphic organizer that lists examples of each device and details their purpose, characteristics, and proper maintenance. Demonstrate proper installation and configuration of each device while using the appropriate media.
  - a. Optical drives
  - b. Combo drives and burners
  - c. Connection types
  - d. Hard drives
  - e. Solid state / flash drives
  - f. RAID types
  - g. Floppy drive
  - h. Tape drive
  - i. Media capacity
- 24) Demonstrate secure networking techniques by designing a simple secure network. For example, show how the various security protocols, technology, and designs protect an organizations network.

### **Basic and Advanced Command Prompts**

- 25) Synthesize information from a range of sources to analyze the various networking commands used to test and examine networks. Using domain-specific terminology, explain to a technical audience the distinguishing features of each command that make one more appropriate for certain types of applications.
- 26) Analyze and research the features and uses of command line utilities to configure and examine networking services and construct a flow chart that a security analyst could reference.

### **Application Security and Host Systems**

- 27) Explore and identify various operating and file systems used in networks. Create a chart to define the pros and cons of how these systems are designed to provide the security necessary in a multiuser environment, citing examples of when each is used.
- 28) Research and describe the most common security threats to computer systems, such as social engineering, malware, phishing, viruses, etc. Investigate and distinguish among the following common prevention methods to secure a computer system. For a given scenario, identify the most applicable best practice to secure a workstation as well as describe methods for data destruction and disposal. Implement these practices and write a justification for each scenario solution. Provide supporting evidence for each solution, drawing on technical texts and industry standards. Prevention methods include:
  - a. Physical security (e.g., lock doors, tailgating, biometrics, badges, key fobs, retinal, etc.)
  - b. Digital security (e.g., antivirus, firewalls, antispyware, user authentication, etc.)
  - c. User education
  - d. Principles of least privilege
- 29) Using news articles and instructional materials, research and report on recent threats and vulnerabilities to systems in networking environments making reference to the top application vulnerabilities and how they are used to exploit systems and networking resources.
- 30) Differentiate between threats and vulnerabilities and what constitutes a network attack and identify how to differentiate between the different types of application attacks. Citing specific examples, create an illustrative guide that outlines major similarities and differences.
- 31) Identify and explain ways to install and configure anti-virus software. Demonstrate the installation of security software design to protect systems on the network. Upon completion of the work, write an explanation and justify the actions by citing supporting evidence from technical manuals and industry standards.

### **Security Administration**

- 32) Research the features and requirements of common security procedures used to protect system resources on a network. Drawing on multiple resources, explain why it is important to know this information when developing a security procedure.
- 33) Identify and describe the differences among various methods to create baseline security measures. Utilizing existing tools on a system, such as the Microsoft Baseline Security Analyzer, outline the steps taken to create a security measure.
- 34) Research the following storage devices and backup media. Create a table or other graphic organizer that lists examples of each device and details their purpose, characteristics, proper maintenance, and methods used to back up and protect data from unauthorized use and access of data.
  - a. Optical drives
  - b. Combo drives and burners
  - c. Connection types
  - d. Hard drives
  - e. Solid state / flash drives
  - f. RAID types



- g. Floppy drive
  - h. Tape drive
  - i. Media capacity
- 35) Demonstrate the methods used to protect against unauthorized use of files. Configure file and folder permissions using both Windows and Linux environments.
- 36) Analyze various protocols and services used by systems for securing them in a network environment. Create a table that lists the purpose and distinguishing features of each protocol and service.

### **Cryptology**

- 37) Drawing on multiple sources (i.e., internet, textbooks, videos, and journals), research the history of cryptology. Create a timeline or infographic, illustrating cryptology's historical evolution from its inception to the present time including but not limited to public key infrastructures, asymmetric and symmetric encryptions. Provide examples drawn from the research to support claims.
- 38) Analyze common methods and use of cryptology to protect data. Compare and contrast general methods used, and explain how their designs and functionalities support the security of data.

### **Standards Alignment Notes**

\*References to other standards include:

- P21: Partnership for 21st Century Skills [Framework for 21st Century Learning](#)
  - Note: While not all standards are specifically aligned, teachers will find the framework helpful for setting expectations for student behavior in their classroom and practicing specific career readiness skills.

# Cybersecurity II

<b>Primary Career Cluster:</b>	Information Technology (IT)
<b>Consultant:</b>	Deborah Knoll, (615) 532-2844, <a href="mailto:Deborah.Knoll@tn.gov">Deborah.Knoll@tn.gov</a>
<b>Course Code(s):</b>	
<b>Prerequisite(s):</b>	<i>Cybersecurity I</i>
<b>Credit:</b>	1
<b>Grade Level:</b>	11
<b>Graduation Requirements:</b>	This course satisfies one of three credits required for an elective focus when taken in conjunction with other Information Technology courses.
<b>Programs of Study and Sequence:</b>	This is the third course in the <i>Cybersecurity</i> program of study.
<b>Aligned Student Organization(s):</b>	SkillsUSA: <a href="http://www.tnskillsusa.com">http://www.tnskillsusa.com</a> Tracy Whitehead, (615) 532-2804, <a href="mailto:Tracy.Whitehead@tn.gov">Tracy.Whitehead@tn.gov</a> Technology Student Association (TSA): <a href="http://www.tntsa.org">http://www.tntsa.org</a> Tracy Whitehead, (615) 532-2804, <a href="mailto:Tracy.Whitehead@tn.gov">Tracy.Whitehead@tn.gov</a>
<b>Coordinating Work-Based Learning:</b>	Teachers are encouraged to use embedded WBL activities such as informational interviewing, job shadowing, and career mentoring. For information, visit <a href="https://tn.gov/education/topic/work-based-learning">https://tn.gov/education/topic/work-based-learning</a> .
<b>Available Student Industry Certifications:</b>	CompTIA Security +
<b>Dual Credit or Dual Enrollment Opportunities:</b>	There are no known dual credit/dual enrollment opportunities for this course. If interested in developing, reach out to a local postsecondary institution to establish an articulation agreement.
<b>Teacher Endorsement(s):</b>	
<b>Required Teacher Certifications/Training:</b>	
<b>Teacher Resources:</b>	<a href="https://tn.gov/education/article/cte-cluster-information-technology">https://tn.gov/education/article/cte-cluster-information-technology</a>

## Course Description

*Cybersecurity II* challenges students to develop advanced skills in concepts and terminology of cybersecurity. This course builds on previous concepts introduced in *Cybersecurity I* while expanding the content to include malware threats, cryptography, wireless technologies and organizational security. Upon completion of this course, proficient students will be demonstrate and understanding of cybersecurity ethical decisions, malware threats, how to detect vulnerabilities, principles of cryptology, security techniques, contingency plan techniques, security analysis, risk management techniques, and advanced methods of cybersecurity .

## Program of Study Application

This program offers a sequence of courses that provides coherent and rigorous content aligned with challenging academic standards and relevant technical knowledge and skills needed to prepare for further education and

cybersecurity-related careers in the Information Technology career cluster. This is the third course in the Cybersecurity program of study. For more information on the benefits and requirements of implementing this program in full, please visit the Information Technology website at <https://tn.gov/education/article/cte-cluster-information-technology>.

## Course Standards

### Legal and Ethical Concepts in Cybersecurity

- 1) Drawing from various resources, analyze current legislation that governs computer related crimes. For example, create a presentation discussing common computer crimes, terms of use, and legal issues such as copyright laws, fair use laws, and trademark ethics pertaining to images, videos, and recorded sounds.
- 2) Using news articles, research and report on current legal cases involving acts of computer crime. For example, research and report on a recent case of computer fraud, piracy, and abuse.
- 3) Consult a variety of sources to analyze methods used to discover method of evidence collection to support legal cases involving computer related crime. Create a presentation highlighting methods used.

### Malware Threats

- 4) Conduct research to determine various forms of malware. Give specific examples and create an infographic highlighting the different types.
- 5) Analyze methods to handle malware, such as how to control access to secured resources and computer resources. Give specific examples of methods that a security analyst can use, like encryption techniques, basic input/output system (BIOS) features, and strategies for dealing with malware.

### Threats and Vulnerabilities

- 6) Analyze and differentiate among various types of attacks on systems and networks. Create a table or other graphic organizer that lists the following types of attacks and details their purposes and characteristics. Different types of attacks can include but are not limited to:
  - a. Virus
  - b. Worms
  - c. Trojans
  - d. Unpatched software
  - e. Password cracking
  - f. Advanced persistent threat
  - g. Reconnaissance/footprinting
  - h. Infiltration
  - i. Network breach
  - j. Network exploitation
  - k. Attack for effects (e.g., deceive, disrupt, degrade, and destroy)
  - l. DoS/DDoS, session hijacking
  - m. HTTP spoofing
  - n. DNS attacks
  - o. Switch attacks
  - p. Man-in-the-middle (MITM) attacks
  - q. Cross site scripting



r. Drive-by-attacks

- 7) Consult a variety of sources to research attack methods and create a report on at least two events. For example, show how social engineering (e.g., baiting, phishing/spear phishing, pretexting/ blagging, tailgating, quid pro quo, etc.) led to the breach of an organization.

### **Principles of Cryptology**

- 8) Research and create an information artifact (e.g., brochure, fact sheet, or narrative) analyzing cryptographic tools, procedures for use, and products including but not limited to: PKI, Certificates, PGP, and Certificate authorities.
- 9) In teams, examine trade journals and research literature from product vendors to develop a simple public key infrastructure to be used by a small business. For example, show how an organization can use digital certificates, encrypted file transfers and email utilizing encryption.
- 10) Investigate and demonstrate the creation of a self-signed certificate for use on a web server by using command line or online tools. For example, create, install, secure, backup, and restore a certificate.

### **Wireless Security Techniques**

- 11) Analyze attack methods on wireless networks. Read and interpret trade journals, assessing the usefulness of each source, to describe the different methods used. For example, cite evidence from trade journals to explain man in the middle, sniffing, and wireless SSID spoofing to explain their unique attack methods.
- 12) Demonstrate the use of wireless security protocols. Drawing on evidence from textbooks and other resources, evaluate the capabilities of WPA, WPA-2, and WEP and the effectiveness of the security protocols and demonstrate how to use them appropriately.

### **Organizational Security Techniques**

- 13) Consult a variety of sources to analyze, define, and demonstrate the use of environmental controls. Instructional material may include textbooks, manuals, websites, video tutorials, and more. For example, show how BIOS sets controls on a system.
- 14) As a class, work collaboratively to develop simple policies that support the operations of security in an organization. For example, create an email security policy that outlines rules regarding responsible technology use.
- 15) Research and analyze security awareness in an organization. Create a table or other graphic organizer that lists the following examples of how to manage user habits and expectations:
  - a. Security policy training and procedures
  - b. Personally identifiable information
  - c. Information classifications
  - d. Data labeling, handling, and disposal
  - e. Compliance with laws, best practices, and standards
  - f. User habits
  - g. Threat awareness
  - h. Use of social networking

### Contingency Planning Techniques

- 16) Synthesize information from a range of sources to analyze and define the impact of security incidents on an organization. For example, describe the various types of incidents including but not limited to malware, intrusion, and other forms of compromise.
- 17) Research and define what is disaster recovery (DR) plan is and how to develop one. For example, develop a step by step guide on how an organization would recover from an incident. The disaster recovery plan should highlight three key aspects: preventive measures, detective measures, and corrective measures. Write a justification that explains to a client why a disaster recovery plan is important.

### Security Analysis Evaluation

- 18) Explore and identify various assessment methods including but not limited to network penetration and vulnerability testing. Create a chart to define how these systems are designed to help identify weak links in a company's cyber security chain and how they provide feedback and recommendations needed in order to address them.
- 19) Identify and explain the uses for security testing tools. Demonstrate and compare the effectiveness of Nessus and Nmap. Write and explanation and justify conclusions by citing supporting evidence from technical manuals vendor resources.
- 20) Demonstrate each of the following concepts:
  - a. Evaluate the patch status of a machine.
  - b. Demonstrate knowledge of packet-level analysis in order to install and view packets.
  - c. Perform secure data destruction (e.g., Secure Erase, BCWipe).

### Advanced Methods of Cybersecurity

- 21) Utilizing prior fundamentals, demonstrate proper secure network configuration and administration. For example, use common tools and design a network utilizing secure protocols, and evaluate the network upon completion. The plan should address, but is not limited, to the following:
  - a. Applying and implementing secure network administration principles.
  - b. Demonstrating knowledge of how network services and protocols interact to provide network communications in order to securely implement and use common protocols.
  - c. Identifying commonly used default network ports.
  - d. Setting up a Network Address Translation (NAT) device.
  - e. Configuring a Virtual Private Network (VPN).
  - f. Configuring a remote access policy Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP).
  - g. Demonstrating 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.
  - h. Locating open ports by completing a port scan.
  - i. Demonstrating the knowledge and use of network statistics (netstat),

## Standards Alignment Notes

\*References to other standards include:

- P21: Partnership for 21st Century Skills Framework for 21st Century Learning
  - Note: While not all standards are specifically aligned, teachers will find the framework helpful for setting expectations for student behavior in their classroom and practicing specific career readiness skills.



# Cybersecurity Practicum

<b>Primary Career Cluster:</b>	Information Technology (IT)
<b>Consultant:</b>	Deborah Knoll, (615) 532-2844, <a href="mailto:Deborah.Knoll@tn.gov">Deborah.Knoll@tn.gov</a>
<b>Course Code(s):</b>	
<b>Prerequisite(s):</b>	<i>Algebra I</i> (0842, 3012) and <i>Cybersecurity II</i>
<b>Credit:</b>	1
<b>Grade Level:</b>	11-12
<b>Graduation Requirements:</b>	This course satisfies one of three credits required for an elective focus when taken in conjunction with other Information Technology courses.
<b>Programs of Study and Sequence:</b>	This is the capstone course in the <i>Cybersecurity</i> program of study.
<b>Aligned Student Organization(s):</b>	SkillsUSA: <a href="http://www.tnskillsusa.com">http://www.tnskillsusa.com</a> Tracy Whitehead, (615) 532-2804, <a href="mailto:Tracy.Whitehead@tn.gov">Tracy.Whitehead@tn.gov</a> Technology Student Association (TSA): <a href="http://www.tntsa.org">http://www.tntsa.org</a> Tracy Whitehead, (615) 532-2804, <a href="mailto:Tracy.Whitehead@tn.gov">Tracy.Whitehead@tn.gov</a>
<b>Coordinating Work-Based Learning:</b>	Teachers who hold an active WBL certificate may offer placement for credit when the requirements of the state board's WBL Framework and the Department's WBL Policy Guide are met. For information, visit <a href="https://tn.gov/education/topic/work-based-learning">https://tn.gov/education/topic/work-based-learning</a> .
<b>Available Student Industry Certifications:</b>	CompTIA Security +
<b>Dual Credit or Dual Enrollment Opportunities:</b>	There are no known dual credit/dual enrollment opportunities for this course. If interested in developing, reach out to a local postsecondary institution to establish an articulation agreement.
<b>Teacher Endorsement(s):</b>	
<b>Required Teacher Certifications/Training:</b>	If students are assigned in work-based learning settings, teachers must attend WBL training and earn the WBL Certificate provided by the Tennessee Department of Education.
<b>Teacher Resources:</b>	<a href="https://tn.gov/education/article/cte-cluster-information-technology">https://tn.gov/education/article/cte-cluster-information-technology</a>

## Course Description

*Cybersecurity Practicum* is a capstone course intended to provide students with the opportunity to apply the skills and knowledge learned in previous *Cybersecurity* courses toward the completion of an in-depth project with fellow team members. Students who have progressed to this level in the program of study take on more responsibilities for producing independent work and managing processes involved in the planning, designing, refinement, and production of cybersecurity applications. Upon completion of the practicum, proficient students will be prepared for postsecondary study and career advancement in cybersecurity, and will be equipped to market their finished product should they choose.

## Work-Based Learning Framework

Practicum activities may take the form of work-based learning (WBL) opportunities (such as internships, cooperative education, service learning, and job shadowing) or industry-driven project-based learning. These experiences must

comply with the Work-Based Learning Framework guidelines established in SBE High School Policy 2.103. As such, this course must be taught by a teacher with an active WBL Certificate issued by the Tennessee Department of Education and follow policies outlined in the Work-Based Learning Policy Guide available online at <https://tn.gov/education/topic/work-based-learning>. The Tennessee Department of Education provides a *Personalized Learning Plan* template to ensure compliance with the Work-Based Learning Framework, state and federal Child Labor Law, and Tennessee Department of Education policies, which must be used for students participating in WBL opportunities.

## **Program of Study Application**

This is the fourth course in the *Cybersecurity* program of study. For more information on the benefits and requirements of implementing this program in full, please visit the Information Technology website at <https://tn.gov/education/article/cte-cluster-information-technology>.

## **Course Standards**

### **Cybersecurity Career Planning**

- 1) Research a company or organization that utilizes cybersecurity applications or specializes in cybersecurity solutions. Companies could range from large software developers, to niche organizations that retain specialists on staff to serve their particular clients' needs. For the chosen company, cite specific textual evidence from the company's literature, as well as available press coverage (if available) to summarize:
  - a. The mission and history of the organization
  - b. Headquarters and organizational structure
  - c. Products or services provided
  - d. Credentials required for employment and how they are obtained and maintained
  - e. Policies and procedures
  - f. Reports, newsletters, and other documents published by the organization
  - g. Website and contact information
- 2) Analyze the requirements and qualifications for various cybersecurity job postings identified from specific company websites or online metasearch engines. Gather information from multiple sources, such as sample resumes, interviews with professionals, and job boards, to determine effective strategies for realizing career goals. Create a personal resume modeled after elements based on the findings above, then complete an authentic job application as part of a career search or work-based learning experience.
- 3) Participate in a mock interview. Prior to the interview, research tips on dress and grooming, most commonly asked interview questions, appropriate conduct during an interview, and recommended follow-up procedures. Upon completion of the interview, write a thank you letter to the interviewer in a written or email format.

### **Professional Ethics and Legal Responsibilities**

- 4) Investigate current issues surrounding cybersecurity and its applications. Explore a range of arguments concerning privacy rights as they relate to the mining of personal data; determine when it is ethical and legal to collect data for profit versus for security purposes. Advance an original argument that debates the pros and cons and summarizes the potential ramifications for clients, users, the public, and one's own personal reputation, drawing on evidence gathered from news media, company policies, and state and federal laws.

- 5) Research a case study involving an ethical issue related to intellectual property rights. Examine a variety of perspectives surrounding the issue, then develop an original analysis explaining the impact of the issue on those involved, using persuasive language and citing evidence from the research. Potential issues include copyright infringement, piracy, plagiarism, art licensing, creative commons, and the state/federal laws that govern them.

### **Course Project**

In teams, students will complete the capstone security assessment to help identify gaps and provide mitigating solutions of a fictitious small and medium-sized business (SMB) that is concerned over their security posture of their business. This assessment should span the various types of tests and attack vectors that students learned about in previous courses in the program of study. The project must provide opportunities for members to experience a high level of interactivity related to the challenges of learning and applying advanced skills in cybersecurity. The project must provide a safe, legal, and ethically sound environment with up-to-date facilities and equipment.

- 6) Research and investigate how policies and procedures are used to define the practices within the business and how are they are used to define the practices within the business as they relate to information security. Create three policies that will help establish a solution to potential security concerns:
  - a. Create an administrative policy, based on this research that employees would need to follow to have access to system resources, or password usage.
  - b. Create a technical policy that defines how a technical control helps to protect an organization. For example, define how the IT department must configure a firewall.
  - c. Create a control policy for the physical controls for the organization. For example, a policy to define the physical access to the IT equipment to help contain unauthorized access to the firewall and or routers.
- 7) Analyze a technical security solution scenario and determine what solution could be deployed to help mitigate an issue and protect the organization against malware infections.
- 8) Test and run a vulnerability assessment on the SMB to determine what vulnerabilities exist on a resource (server, network device, computer, etc.) using Nessus. Students will run a scan on a computer find the vulnerabilities, and preform the mitigating steps to remove the identified vulnerabilities.

### **Communication of Project Results**

- 9) Upon completion of the practicum, develop a technology-enhanced presentation showcasing their findings and solutions, highlights, challenges, and lessons learned from the experience to a small volunteer panel of professionals that could serve as the fictitious business owners. The presentation should be delivered orally, but supported by relevant graphic illustrations, such as diagrams, flowcharts, and/or market data on the target users. Prepare the presentation in a format that could be presented to both a technical and a non-technical audience, as well as for a career and technical student organization (CTSO) or CyberPatriot competitive events.

### **Portfolio**

- 10) Create a portfolio, or similar collection of work, that illustrates mastery of skills and knowledge outlined in the previous courses and applied in the practicum. The portfolio should reflect thoughtful assessment and evaluation of the progression of work involving the application of steps of the design process, as outlined by the instructor. The following documents will reside in the student's portfolio:
  - a. Personal code of ethics



- b. Career and professional development plan
- c. Resume
- d. Project proposal with supporting documents
- e. List of responsibilities undertaken through the course
- f. Examples of visual materials developed and used during the course (such as drawings, models, presentation slides, videos, and demonstrations)
- g. Marketing plan
- h. Description of technology used, with examples if appropriate
- i. Periodic journal entries reflecting on tasks and activities
- j. Feedback from instructor and/or supervisor based on observations

### **Standards Alignment Notes**

\*References to other standards include:

- P21: Partnership for 21st Century Skills [Framework for 21st Century Learning](#)
  - Note: While not all standards are specifically aligned, teachers will find the framework helpful for setting expectations for student behavior in their classroom and practicing specific career readiness skills.

# Mobile App Development

<b>Primary Career Cluster:</b>	Information Technology
<b>Consultant:</b>	Deborah Knoll, (615) 532-2844, <a href="mailto:Deborah.Knoll@tn.gov">Deborah.Knoll@tn.gov</a>
<b>Course Code(s):</b>	
<b>Prerequisite(s):</b>	<i>Algebra I</i> (0842, 3102), <i>Computer Science Foundations</i> (6095) Coding I (6098)
<b>Credit:</b>	1
<b>Grade Level:</b>	11
<b>Graduation Requirements:</b>	This course satisfies one of three credits required for an elective focus when taken in conjunction with other Information Technology courses.
<b>Programs of Study and Sequence:</b>	This is an option for the third course in the <i>Programming &amp; Software Development (Coding)</i> program of study.
<b>Aligned Student Organization(s):</b>	SkillsUSA: <a href="http://www.tnskillsusa.com">http://www.tnskillsusa.com</a> Tracy Whitehead, (615) 532-2804, <a href="mailto:Tracy.Whitehead@tn.gov">Tracy.Whitehead@tn.gov</a> Technology Student Association (TSA): <a href="http://www.tntsa.org">http://www.tntsa.org</a> Tracy Whitehead, (615) 532-2804, <a href="mailto:Tracy.Whitehead@tn.gov">Tracy.Whitehead@tn.gov</a>
<b>Coordinating Work-Based Learning:</b>	Teachers are encouraged to use embedded WBL activities such as informational interviewing, job shadowing, and career mentoring. For information, visit <a href="https://tn.gov/education/topic/work-based-learning">https://tn.gov/education/topic/work-based-learning</a> .
<b>Available Student Industry Certifications:</b>	
<b>Dual Credit or Dual Enrollment Opportunities:</b>	There are no statewide dual credit/dual enrollment opportunities for this course. If interested in establishing a local opportunity, reach out to a local postsecondary institution.
<b>Teacher Endorsement(s):</b>	037, 041, 055, 056, 057, 152, 153, 203, 204, 311, 434, 435, 436, 474, 475, 476, 477, 582, 595, 740, 742
<b>Required Teacher Certifications/Training:</b>	All endorsements except for 742 will require the equivalent of twelve semester hours of computer course work including at least six hours of programming language.
<b>Teacher Resources:</b>	<a href="https://tn.gov/education/article/cte-cluster-information-technology">https://tn.gov/education/article/cte-cluster-information-technology</a>

## Course Description

*Mobile App Development* is a course intended to teach students the basic concepts and skills of mobile app design. The course places an emphasis on the history of mobile technologies, design and development methodologies, code for mobile applications, application lifecycles, APIs, mobile device controls, user interfaces, deployment, publishing for mobile devices, developer tools, and career development. Upon completion of this course, proficient students will be demonstrate and understanding of mobile app development concepts.

## Program of Study Application

This program offers a sequence of courses that provides coherent and rigorous content aligned with challenging academic standards and relevant technical knowledge and skills needed to prepare for further education and mobile app design-related careers in the Information Technology career cluster. This is a third course option in the



*Programming & Software Development (Coding) program* of study. For more information on the benefits and requirements of implementing this program in full, please visit the Information Technology website at <https://tn.gov/education/article/cte-cluster-information-technology>.

## **Course Standards**

### **Introduction to Mobile Technologies**

- 1) Using news articles and instructional materials, investigate key milestones in the development of how mobile technologies came to be. Create and present a document and/or illustration depicting the timeline of development that led current major mobile platforms and describe the effects upcoming mobile platforms may have on mobile technologies. For example, students should include:
  - a. Early Applications (calculators, basic arcade games, calendars)
  - b. Wireless Application Protocol (WAP) and Wireless Markup Language
  - c. Proprietary Mobile Platforms (Palm OS, Java Micro Edition, iPhone iOS, Android)
  - d. Commercialization of Applications
  - e. 'Mobile First' Approach
- 2) Investigate the different physical capabilities of a mobile device including: identifying different device sensors, built-in hardware, and the specifications of the camera. Create a chart that outlines the physical capabilities of a particular mobile device.
- 3) Compare and contrast the benefits, features, Application Programming Interface (API's), number of touch points, networking, energy savings, and typical applications of common modern mobile devices. Craft an argument to defend the choice of a certain key features, developing claim(s) and counterclaim(s) with specific textual evidence and reasoning.

### **Career Exploration**

- 4) Explore career opportunities, trends, and requirements related to careers in mobile applications such as developer, architect, UI designer, interaction designer, product manager, and more. Produce a career pathways chart or other graphic detailing the aptitudes and training required (including personal aptitudes, postsecondary credentials, and licensing) for careers of interest.
- 5) Research educational opportunities to determine programs, degrees, and training availability to improve job prospects in mobile application development. Synthesize findings into a presentation, document, spreadsheet data/chart, or other format highlighting the type of opportunity, focus, time commitment, cost, and outcomes.

### **Mobile Applications Overview**

- 6) Investigate the size and scope of the mobile application market including the rising popularity of mobile apps, and implications for various industries (gaming, location based navigation services, factory automation, banking, online shopping). For instance, investigate the growth of mobile medical apps and discuss security and privacy concerns and reliance on the internet. Discuss the global market and availability and use of mobile applications in developing countries and emerging economies.
- 7) Differentiate between types of mobile applications, including native applications, web applications, and hybrid applications. Identify pros and cons of each type and instances where each type would be the best suited for a particular task.



- 8) Identify major categories of mobile applications: social networking, books, business and finance, lifestyle, travel, navigation, productivity and as a class, create, review, and revise a presentation explaining the different categories by citing resources and identifying examples of mobile applications.
- 9) Understand privacy needs in the development of mobile applications and explore the role security considerations play in development. Research examples of how security and privacy leaks in mobile applications have affected users and society. Students should evaluate a mobile application in terms of meeting privacy needs, legal and intellectual property requirements, and security considerations (such as preventing attacks from malicious hackers, building secure applications, preventing data leaks, secure mobile transactions for in-app purchases).
- 10) Define Device Application Programming Interface (DAP) and discuss advantages/disadvantages for utilizing API in mobile application development. List types of common DAPs available to developers (mapping/geolocation, device orientation, vibration, forms, media, etc.) and provide an example of an application that utilizes each type.
- 11) Explore programming languages used in development of mobile applications, including Objective-C, Swift, C#, Java, Ruby, and JavaScript. Demonstrate an understanding why apps use different languages for development and discuss cross-platform app design.
- 12) Identify the most commonly used developer tools and platforms. Communicate this information and engage each other effectively using appropriate wiki's and blogs to support individual learning and contribute to the learning of others.

### **Mobile Applications Design**

- 13) Describe elements of mobile application design which includes designing for multiple devices, screen sizes, browsers, and operating systems. Discuss how developers design applications for the best user experience.
- 14) Identify and be able to apply the principles of user interface design, including:
  - Why designing applications that are intuitive and user-friendly is important
  - How design can make common tasks easy
  - How to design applications for users with disabilities
  - How to handle user errors and provide feedback
- 15) Apply user interface design criteria, such as navigating the app, user input, gestures, orientation, communication (alerts, confirmations, and feedback), first impression of the polish of the design, launch time, to critique common user interfaces in mobile applications. Discuss how the design can motivate or demotivate a user. Compare and contrast various applications based on usability.

### **Mobile Application Development**

- 16) Demonstrate an understanding of the mobile application life cycle and the iterative nature of a lifecycle. Understand and use steps for designing a good software product.
- 17) Develop an idea into a project plan then write pseudocode and construct a flowchart for a process before starting to develop the program code.
- 18) Develop a mobile application and write original program code using basic Object-oriented programming (OOP) concepts including:



- a. Variables
  - b. Methods
  - c. Control structures
  - d. Data structures
  - e. User input
- 19) When writing program code, demonstrate an ability to evaluate code, identify errors, and troubleshoot bugs.
- 20) Create a mobile application that incorporates the use of phone controls and a custom control. The application should display content, incorporate notifications, and use tasks to enhance functionality. For example, create a basic time management app.
- 21) Utilizing the application developed in the previous standard (or another), enhance the application by incorporating user interface design standards and guidelines, including optimizing the layout, designing screen orientation options, colors, transparency.
- 22) Integrate images and media in the application developed in the previous standards. Students may create appropriate art, develop audio, and create applications animations or utilize pre-existing media.

#### **Deployment**

- 23) Demonstrate an understanding for how to deploy a mobile application to the marketplace, including marketplace submission rules and creating the deployment package. Advanced students might deploy an application.

#### **Project Management**

- 24) As a team during an extended project, develop a platform-specific mobile application that conforms to acceptable coding standards, including organization and comments and contains appropriate graphics, text, audio, and animations. The team should utilize project management techniques to develop a plan with considerations for cost and time. Additionally, the team should create a design document that details the application, the problem it solves, and its core features.

#### **Standards Alignment Notes**

\*References to other standards include:

- P21: Partnership for 21st Century Skills [Framework for 21st Century Learning](#)
  - Note: While not all standards are specifically aligned, teachers will find the framework helpful for setting expectations for student behavior in their classroom and practicing specific career readiness skills.



# Computer Science Foundations

<b>Primary Career Cluster:</b>	Information Technology (IT)
<b>Consultant:</b>	Deborah Knoll, (615) 532-2844, <a href="mailto:Deborah.Knoll@tn.gov">Deborah.Knoll@tn.gov</a>
<b>Course Code:</b>	6095
<b>Prerequisite(s):</b>	None
<b>Credit:</b>	1 credit for core and two focus areas. 2 credits for all 29 standards.
<b>Grade Level:</b>	9
<b>Graduation Requirement:</b>	This course satisfies one or two of three credits required for an elective focus when taken in conjunction with other IT courses.
<b>Programs of Study and Sequence:</b>	This is the first course in the <i>Networking Systems, Programming and Software Development (Coding)</i> , and <i>Web Design</i> programs of study.
<b>Aligned Student Organization(s):</b>	Future Business Leaders of America (FBLA) <a href="http://www.fblatn.org">www.fblatn.org</a> Steven Mitchell, (615) 532-2829, <a href="mailto:Steven.Mitchell@tn.gov">Steven.Mitchell@tn.gov</a> SkillsUSA: <a href="http://www.tnskillsusa.com">http://www.tnskillsusa.com</a> Tracy Whitehead, (615) 532-2804, <a href="mailto:Tracy.Whitehead@tn.gov">Tracy.Whitehead@tn.gov</a> Technology Student Association (TSA): <a href="http://www.tntsa.org">http://www.tntsa.org</a> Tracy Whitehead, (615) 532-2804, <a href="mailto:Tracy.Whitehead@tn.gov">Tracy.Whitehead@tn.gov</a>
<b>Coordinating Work-Based Learning:</b>	Teachers who hold an active work-based learning (WBL) Certificate issued by the Tennessee Department of Education may offer appropriate student placement. To learn more, please visit: <a href="https://tn.gov/education/topic/work-based-learning">https://tn.gov/education/topic/work-based-learning</a> .
<b>Available Student Industry Certifications:</b>	CompTIA IT Fundamentals
<b>Dual Credit or Dual Enrollment Opportunities:</b>	There are no known dual credit/dual enrollment opportunities for this course. If interested in developing, reach out to a local postsecondary institution to establish an articulation agreement.
<b>Teacher Endorsement(s):</b>	037, 041, 055, 056, 057, 152, 153, 203, 204, 311, 434, 435, 436, 474, 475, 476, 477, 582, 595, 740, 742
<b>Required Teacher Certifications/Training:</b>	None
<b>Teacher Resources:</b>	<a href="https://tn.gov/education/article/cte-cluster-information-technology">https://tn.gov/education/article/cte-cluster-information-technology</a>

## Course Description

*Computer Science Foundations* (CSF) is a course intended to provide students with exposure to various information technology occupations and pathways such as Networking Systems, Programming and Software Development (Coding), Web Design, and Cybersecurity. As a result, students will complete all

core standards, as well as standards in two of four focus areas. Upon completion of this course, proficient students will be able to describe various information technology (IT) occupations and professional organizations. Moreover, they will be able to demonstrate logical thought processes and discuss the social, legal, and ethical issues encountered in the IT profession. Depending on the focus area, proficient students will also demonstrate an understanding of electronics and basic digital theory; project management and teamwork; client relations; causes and prevention of Internet security breaches; and writing styles appropriate for web publication. Upon completion of the CSF course, students will be prepared to make an informed decision about which Information Technology program of study to pursue

The following implementation options are encouraged:

- 1 credit for core and two focus areas (listed below)
- 2 credits for all 29 standards

Core standards are required for both one and two credit implementation options.

**Core standards:** 1, 2, 3, 7, 8, 9, 23

**Focus Areas**

Networking Systems:

Programming & Software Development:

Web Design:

Cybersecurity:

**Standards**

4, 5, 6, 12, 13, 16, 17

16, 17, 27, 28, 29, 30

10, 11, 14, 15, 18, 19, 20, 21, 22

13, 24, 25, 26

**Program of Study Application**

This is the first course in the *Networking Systems, Programming and Software Development (Coding), Web Design, and Cybersecurity* programs of study. For more information on the benefits and requirements of implementing these programs in full, please visit the Information Technology website at <https://tn.gov/education/article/cte-cluster-information-technology>.

**Course Standards**

**Safety**

- 1) Accurately read, interpret, and demonstrate adherence to safety rules, including (1) rules published by the National Science Teachers Association (NSTA), (2) rules pertaining to electrical safety, (3) Internet safety, (4) Occupational Safety and Health Administration (OSHA) guidelines, and (5) state and national code requirements. Be able to distinguish between rules and explain why certain rules apply.
- 2) Identify and explain the intended use of safety equipment available in the classroom. For example, demonstrate how to properly inspect, use, and maintain safe operating procedures with tools and equipment.

**Electronics and Basic Digital Theory**

- 3) Demonstrate understanding of electrical circuits and devices, and relate to the physical laws (such as Ohm's Law and power laws) that govern behaviors of electrical circuits and devices. Accurately apply these physical laws to solve problems. For example, calculate the resistance of a DC circuit with a given DC voltage and current.
- 4) Assemble the required connections of electronic test equipment to properly test the operation of basic electronic circuit behavior and performance, using equipment such as a digital multimeter. For example, demonstrate the proper use of a digital multimeter by measuring resistance of a circuit in a typical computer system; compare this finding by calculating the resistance given the voltage and current.
- 5) Distinguish between the binary and hexadecimal counting systems. Using appropriate units, provide examples of each system and identify specific instances when IT professionals rely on them.
- 6) Explain the functions of gates in logic circuits (e.g., AND, OR, NOT). For example, construct a truth table for the seatbelt warning light in an automobile.

### **Career Exploration**

- 7) Research various occupations in information technology industries, such as programmers, web designers, webmasters, networking administrators, computer systems administrators, telecommunications line installers, and an Information Security Analyst. Compose an informative table or chart that includes the following: work activities typically performed, tools and technology used, nature of work environment, and the knowledge and skills needed for success.
- 8) Explore various professional societies related to information technology and identify the services and benefits provided by each member. Create a table that lists their purposes, benefits to membership, and any certifications affiliated with the organization. For example, investigate the Institute for Electrical and Electronics Engineers (IEEE), Computing Technology Industry Association (CompTIA), and the Association for Computing Machinery (ACM).

### **Overview of the Internet**

- 9) Drawing on multiple sources (i.e., internet, textbooks, videos, and journals), research the history of the Internet. Create a timeline or infographic, illustrating the Internet's historical evolution from its inception to the present time. Discuss the needs that led to the creation of the Internet; discuss both the benefits and disadvantages of the Internet to society, as well as potential implications for the future. Provide examples drawn from the research to support claims.

### **Overview of Operating Systems**

- 10) Drawing on multiple sources (i.e., internet, textbooks, videos, and journals), research the history and development of operating systems (e.g., Microsoft Windows, Linux, UNIX). Create a presentation, illustrating their historical evolution, from their inceptions to the present, citing information found in research. Compare and contrast the general capabilities of a variety of operating systems, and explain how their designs and functionalities have improved over time.

### **Terminology and Concepts**

- 11) Demonstrate an understanding of basic web terminology and concepts. Practice explaining these terminologies and concepts by creating methods to help students learn and remember the information. For example, students should be able to explain the purpose of terminology such as server, domain name system (DNS), internet service provider (ISP), hardware and software connective devices, cloud computing, remote access protocols, map protocols, content management systems (CMS), cascading style sheets (CSS), and social networking terms.
- 12) Demonstrate a basic understanding of computer hardware components. Identify these components using pictures or actual models and briefly explain the function of each. Components should include, but are not limited to:
  - a. Hardware used for input and output
  - b. Hardware inside the computer case
  - c. Motherboard
  - d. Processor and the chipset
  - e. Storage devices (e.g., primary, secondary)
  - f. Expansion cards
  - g. Electrical system
- 13) Demonstrate a basic understanding of computer networking. For example, explain the types of networks and what a client-server environment is.

#### **Keyboard Shortcuts**

- 14) Identify, explain, and demonstrate the use of common keyboard shortcuts. Create a quick reference guide that would be user-friendly for a novice web designer. For example, students may create a multiple column table showing keyboard shortcuts for navigation, text editing, and text formatting. The table would identify which shortcuts are applicable to using Windows versus Mac OS.

#### **Introduction to Logical Thought Process**

- 15) There are different versions of the web design and development process. For example, most versions of the web design and development process involve project definition, site structure, visual design, site development, testing, refining, and launch. Using various resources, research, identify, and explain the steps involved in the process. As a class, develop an agreed-upon framework for applying the logical thought process to web design projects in the form of a flowchart or logic model, justifying the reasoning behind each step. Explain why it is an iterative process and always involves refinement.
- 16) Research, identify, and describe the specific activities involved at each step of the troubleshooting process, including but not limited to: 1) gather information from the user or operator and back up data, 2) verify the problem exists, 3) isolate the cause of the problem and generate alternative solutions, 4) plan a solution and resolve the problem, 5) verify that the problem was resolved and prevent a future occurrence, and 6) document findings, resolution, and preventative maintenance plan. Explain why it is important to document the process throughout.
- 17) Demonstrate an understanding of flowcharts and know what various symbols mean. Identify a problem that a programmer would solve using the logical thinking process, and create a flowchart that would guide the code development. For example, create a flowchart that incorporates at least three decisions, or paths, to solve a problem.

### **Teamwork & Project Management**

- 18) Explore how teams are formed to complete and manage web design and development projects. Using the information gained from research, identify and explain various roles and responsibilities for members of a web design and development team. Include why teams are more efficient than individuals in the web design and development process. Present the findings to classmates.
- 19) Synthesize common principles and templates for successful project management. Explain, using examples, why strong management skills are important in the web design and development process.

### **Client Relations**

- 20) Research and identify the skills that are required to communicate effectively with a client. Develop a questionnaire that would be used to determine the needs of a client for a prospective web development project. Using the questionnaire, conduct mock client interviews with classmates and provide each other with constructive feedback to revise the questionnaire and process.

### **Writing and Editing for Web Publication**

- 21) As a team, list primary rules to guide writing content that is appropriate for a web site publication. Apply these rules to a variety of web-based writing assignments throughout the course. For example, develop and maintain a blog throughout the course to practice appropriate writing techniques and style for web publication.
- 22) Given a specific client's vision, create a simple web site using a content management system (CMS) such as WordPress. Follow the multistep process to download the software application of choice, and demonstrate how to upload and store files. Practice proofreading and critiquing other classmates' sites, and provide constructive feedback on one another's writing and layout design.

### **Social, Legal, and Ethical Issues**

- 23) Drawing on multiple sources (i.e., internet, textbooks, videos, and journals), research the various social, legal, and ethical issues encountered by IT professionals. Using these findings, identify the roles and responsibilities one must consider while developing a prospective project or addressing an IT problem. For example, web developers and programmers must apply copyright laws and understand uses of open source software.

### **Cybersecurity**

- 24) Using various sources (i.e., internet, textbooks, videos, and journals), research and identify reasons as to why data security should be a priority to technology professionals through demonstrating an understanding of information security fundamentals on Confidentiality, Availability, and Integrity.
- 25) Demonstrate an understanding of the various security breaches that can occur with the Internet. Prepare a text explaining enterprise-level security, the purpose of encryption, and the protocols that can be implemented to secure web sites. Evaluate personal privacy issues versus employers' rights to regulate computing resources.



- 26) Identify various security practices for computer and network systems, such as how to control access to secured resources and computer resources. Give specific examples of methods that an administrator can use, like encryption techniques, basic input/output system (BIOS) features, and strategies for dealing with malware.

### **Organization of Materials**

- 27) Understand and demonstrate the effective use of file and folder management techniques to maintain directory structure for a web site. Describe the most efficient methods for digital file management, including the use of site root and subfolders for assets (e.g., images, templates, CSS).

### **Programming**

- 28) Explore and identify various languages, such as Python, HTML, PHP, C++, Visual Basic, Java, JavaScript, and C#. Explain how programmers use these languages to solve a variety of IT problems, furnishing examples of how they are applied.
- 29) Using various resources, research, identify, and explain the steps involved in the software development life cycle, including but not limited to: planning, designing, coding, testing, deployment, and maintenance. Explain why it is an iterative process and always involves refinement.
- 30) Demonstrate an understanding of how batch files function within a programming environment. Identify common commands to create code for batch files (e.g., title, echo, echo off, pause, CLS, ipconfig, and ping). For example, list various scenarios for using batch files to complete specific programming tasks. Create and execute batch file code to perform one of the tasks identified.

### **Standards Alignment Notes**

\*References to other standards include:

- P21: Partnership for 21st Century Skills [Framework for 21st Century Learning](#)
  - Note: While not all standards are specifically aligned, teachers will find the framework helpful for setting expectations for student behavior in their classroom and practicing specific career readiness skills.