

Florida Department of Education

CURRICULUM FRAMEWORK

Program Title: IT Security
 Occupational Area: Business Technology Education
 Program Classification: PSV
 Program Type: AS* or AAS*
 Grade Level: College Credit
 CIP Number: 0506120106 AAS
 1506120106 AS
 Length: 63 College Credits
 SOC Code: 15-1061 Database Administrators

- I. MAJOR CONCEPTS/CONTENT: The purpose of this program is to prepare students for employment as Database Security Professionals and E-Commerce Security Professionals, or to provide supplemental training for persons previously or currently employed in occupations such as E-commerce Developers, E-commerce Coordinators, E-commerce Web Site Support Specialists, Database Administrators, Database Architects, Database Developers, or Enterprise Specialist. Elements from this program could also be used to supplement training programs for Web Technicians, Internet/Intranet Administrators, Web Administrators, and Internet Support Specialists. The content prepares individuals to work in Internet, intranet, extranet, and enterprise environments; installing, configuring, designing, and managing secure database and E-commerce resources.
- II. LABORATORY ACTIVITIES: Laboratory activities are an integral part of this program and include the use of computers, computer software, and networking/internetworking hardware and software.
- III. COMPLEMENTARY SOFTWARE AND EQUIPMENT: The following tools and equipment are required for this program: servers, workstations, peripheral devices, network operating systems software, Web server software, email server software, database server and client software, e-commerce software, hacking toolkits, Web browser software, FTP client software, Web authoring software, firewall software, proxy servers, backup software and hardware, data communications tools, LAN and WAN network infrastructures, routers and switches, communication servers, remote access software and hardware, VPN software and hardware, anti-virus software, network analyzers, network monitors, packet sniffers and scanners, penetration testing and reconnaissance software, quantitative analysis software, Web analysis software, database management software, and encryption software.
- IV. INSTRUCTOR QUALIFICATIONS: Preferred: Masters Degree in Field or Masters degree and 18 hours in Management Information Systems, Computer Programming, Database Management Systems, Information Studies, or Information Science. Experience working in networking related fields such as Network Security Analyst, Database Administrator, Internetwork Systems Administrator, Webmaster, Web Programming, WebDBA, or related area. Industry Certification in appropriate area. Minimum: Associate Degree and two or more years of related work experience.

- V. WORK/LEARN CYCLES: The cooperative method of instruction including internship and apprenticeship is strongly recommended for this program. Whenever the cooperative method is offered, the following is required for each student: a training plan (signed by the student, teacher and employer) which includes instructional objectives and a list of on-the-job and in-school learning experiences; a work station which reflects equipment, skills and tasks that are relevant to the occupation which the student has chosen as a career goal. It is recommended that the student receive monetary compensation, as well as credit, for work performed.
- VI. DISTANCE LEARNING DELIVERY: Effective distance learning in technical degree programs is sometimes difficult to accomplish due to the need for student participation in skills activities as part of the curriculum. Complete programs, however, can be offered successfully for those students in which time and geographical distance are restricting factors. This is accomplished by using distance-learning materials for concept/theory mastery and skills labs that allow the student to complete the skill objectives of the curriculum across a variety of schedules. A distinction should be made between distance learning products that contain conceptual and theoretical content ("content products") as opposed to those that may serve merely as a framework for such content ("delivery products"). Many products contain both elements, but each product should be examined with this distinction in mind. Presently available delivery products offer a variety of delivery mechanisms that utilize both synchronous and asynchronous tools to allow interaction with instructors, fellow students, and practicing professionals. A good delivery product should include the following components: An online grade book and progress status report; grade reporting tool for students to view grades; quiz development tool; administration tools, such as grade distribution status reports and other statistical data; backup, download, and upload tools; student and Web page access tracking; glossary and index tools; assignment drop-box; email and discussion tools; chat room and white board; capability to incorporate multimedia; student presentation component; easily accessible Help files; and course announcement tools. Two of the most popular of these programs are Blackboard and WebCT. Many studies and comparative evaluations of distance learning products have been performed over recent years and results are often published on the Web. A list of web sites containing information related to this issue can be found in Appendix A.

The Florida Community College Distance Learning Consortium (web site at www.distancelearn.org) contracts each year with a number of vendors offering a computer based training (CBT) in a broad spectrum of information technology topics. Florida community colleges can select courses covering those topics appropriate for their programs to enhance both traditional and online offerings within this degree. Three major CBT products that contain conceptual and theoretical content related to this program have been documented and compared in the appendices at the end of this framework. The products reviewed were: Course Technology (www.course.com) NetG (www.netg.com) SmartForce (www.smartforce.com) The appendices include a comparative analysis of each products basic attributes, listings of the content modules offered by each of these products, and a mapping of this framework's outcomes to these modules.

VII. MODEL FOR ACCELERATED WORKFORCE EDUCATION: Instead of the traditional sixteen-week course model, classes could be given in an accelerated eight-week model. These classes would meet five hours per week. Due to the technical nature of these classes, each class should meet for a minimum of two and one-half hours per session. Another accelerated option available is a four-week model with each course meeting ten hours per week, preferably two hours per day, five days a week. A hybrid model combining instructor-led training and online Internet modules is another alternative.

VIII. SPECIAL NOTES: Industry certifications have become an important measure of success in the information technology fields. Whenever possible, current industry certifications should be addressed within the program.

The traits and attitudes necessary for success within this program include: creativity, persistence, tenacity, logic/reasoning ability, technical aptitude, flexibility, detail-orientation, stamina, forthrightness, honesty, vision, solutions-orientation, ethical, ability to work under stress, open-minded, eager to learn, analytic, dependability, and the ability to anticipate and detect security violations.

Future Business Leaders of America (Secondary), Phi Beta Lambda (Postsecondary), and Business Professionals of America (BPA) are the appropriate Career Student Organizations (CSO) for providing leadership training and for reinforcing specific career and technical skills. Career Student Organizations, when provided, shall be an integral part of the career and technical instructional program, and the activities of such organizations are defined as part of the curriculum in accordance with Rule 6A-6.065, FAC.

Federal and state legislation requires the provision of accommodations for students with disabilities to meet individual needs and ensure equal access. Adult students with disabilities must self-identify and request such services. Students with disabilities may need accommodations in such areas as instructional methods and materials, assignments and assessments, time demands and schedules learning environment, assistive technology and special communication systems. Documentation of the accommodations requested and provided should be maintained in a confidential file.

This degree requires the inclusion of the minimum number of credits of general education coursework required by SACS.

General Education Requirements (credits as required by SACS):

- Demonstrate communication skills. (English)
- Perform problem solving activities and math computations. (Math)
- Develop human relations skills. (Humanities)
- Demonstrate knowledge of Physical Science. (Science)
- Demonstrate knowledge of Social Science. (Social Science)

Intended Outcomes - After successfully completing this program, the student will be able to:

Foundation Courses:

Computer/Networking Core

- 01.0 Demonstrate an understanding of computer hardware.
- 02.0 Demonstrate an understanding of networked environments, hardware, and software.
- 03.0 Install and configure secure network systems software and utilities.
- 04.0 Demonstrate proficiency with Internet structure, organization, and navigation.
- 05.0 Demonstrate an understanding of network access control systems and methodology.
- 06.0 Describe cryptography concepts, standards, and applications.
- 07.0 Perform telecommunications and network security activities.

Database Core

- 08.0 Demonstrate an understanding of Database Management Systems.
- 09.0 Perform administrative tasks related to database security.

E-commerce Core

- 10.0 Demonstrate an understanding of E-commerce.
- 11.0 Perform tasks related to e-commerce security.
- 12.0 Perform Web site management activities.

Operations Core

- 13.0 Design and implement physical security measures.
- 14.0 Perform operations and security management practices.
- 15.0 Employ applications and systems development security techniques.
- 16.0 Develop business continuity and disaster recovery plans
- 17.0 Describe ethical issues, pertinent laws, and how to conduct investigations.

Professional Core

- 18.0 Perform general organizational computing workplace competencies.
- 19.0 Perform project planning and management activities.
- 20.0 Perform documentation and technical reference activities.
- 21.0 Demonstrate employability skills.
- 22.0 Demonstrate professional development skills 60

July 2007

Florida Department of Education

Student Performance Standards

Program Title: IT Security

Foundation Courses

01.0 Demonstrate an understanding of computer hardware-The student will be able to:

01.01 Describe multiple numbering systems used to represent instructions and data, including binary, octal, decimal, and hexadecimal.

01.02 Identify the architecture of major hardware platforms.

01.03 Describe the functions of major hardware components of a computer system.

01.04 Discuss the potential impact of emerging hardware technologies.

01.05 Perform preventive maintenance tasks on microcomputer systems.

01.06 Set up and configure computer systems and peripherals.

01.07 Configure the Basic Input/Output System (BIOS) of a computer system.

01.08 Install and configure storage devices, controllers, and network interfaces.

02.0 Demonstrate an understanding of networked environments, hardware, and software. The student will be able to:

02.01 Discuss fundamental network concepts such as topology, protocols, architecture, and internetworking

02.02 Define all layers in the Open Systems Interconnect (OSI) and Transmission Control Protocol/Internetworking Protocol (TCP/IP) network protocol models

02.03 Discuss the nature of Internetworking Protocol (IP) addresses and Media Access Control (MAC) addresses, and mapping between protocol addressing schemes

02.04 Describe the functions and hardware requirements for current popular network servers for such services as: Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), e-mail, the

- World Wide Web (WWW), proxy, etc.)
- 02.05 Describe the major functions and hardware requirements of network client hardware components
- 02.06 Describe current link technologies such as twisted-pair, coaxial, fiber optic, and wireless
- 02.07 Describe the major functions of network connectivity hardware, such as hubs, repeaters, bridges, routers, switches, and gateways
- 02.08 Describe the function of network storage devices and other peripherals such as a Redundant Arrays of Inexpensive Disks (RAID) and CD-ROM towers
- 03.0 Install and configure secure network systems software and utilities-The student will be able to:
- 03.01 Install and configure current leading system software, drivers, and service packs.
- 03.02 Install, configure and set up a proxy server and a gateway.
- 03.03 Discuss the functions of authentication protocols and Virtual Private Networks (VPNs).
- 03.04 Configure e-commerce servers and database servers.
- 03.05 Install and configure mailing list servers, chat servers, and newsgroup servers.
- 03.06 Use system software to perform routine maintenance tasks such as backup, hard drive defragmentation, etc.
- 03.07 Install and configure a secure desktop client operating system.
- 03.08 Describe modifications necessary to an operating system (such as modifying parameters, how to handle conflicting interrupts, etc.) when installing, configuring, and upgrading typical applications software.
- 03.09 Install and configure client software for network-based applications such as e-mail, Web browsing, terminal emulation, file transfer, group conferencing, database, etc.
- 03.10 Install and configure current popular network servers for such services as: Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), e-mail, the World Wide Web (WWW), proxy service, etc.).
- 04.0 Demonstrate proficiency with Internet structure, organization, and navigation-The student will be able to:
- 04.01 Describe Internet structure and administration, including such topics as Requests For Comments (RFCs) and the Domain Name System (DNS).
- 04.02 Describe common Internet services and port numbers.
- 04.03 Demonstrate the use of internetworking protocols, including: Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), e-mail protocols such as Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP3), Telnet, etc.).
- 04.04 Differentiate between push and pull technologies.
- 04.05 Demonstrate the use of typical remote access mechanisms such as Telnet.
- 04.06 Describe the data format and proprietary nature of commonly

used Internet file types.

04.07 Demonstrate use of Internet clients and services such as e-mail, Web browsers, search engines, newsgroups, mailing lists, chat rooms, file transfer clients, etc.

05.0 Demonstrate an understanding of network access control systems and methodology-The student will be able to:

05.01 Specify by access control mechanisms what users can do, which resources they can access, and what operations they can perform on a system

05.02 Compare and contrast several access control techniques, including access control

lists, discretionary, mandatory, lattice-based, rule-based, and role-based access control

05.03 Administer computer, group, and user accounts

05.04 Manage policies, rights, permissions, and passwords for users and/or groups of users

05.05 Demonstrate an understanding of various access control models including the Bell-LaPadula, Biba, Clark and Wilson, and State Machine Models

05.06 Oversee password and PIN selection, management, and control

05.07 Demonstrate an understanding of alternative methods to identification and authentication, including characteristic-based or biometric techniques, tokens, tickets, one-time passwords, and single sign-on techniques

05.08 Implement centralized/remote authentication access controls such as RADIUS and TACACS

05.09 Implement and manage decentralized access controls such as domains and trusts relationships

05.10 Analyze methods of server attack, including brute force, denial of service, spoofing, spamming, sniffers, hackers, and crackers

05.11 Demonstrate an understanding of the different types of intrusions and the different methods of intrusion detection, including data extraction, sampling, recognition and traffic analysis

05.12 Monitor the network using various forms of intrusion detection resources to detect attacks

05.13 Investigate audit trails for signs of network intrusions

05.14 Perform penetration testing to find weaknesses in the access control systems

06.0 Describe cryptography concepts, standards, and applications-The student will be able to:

06.01 Demonstrate an understanding of the encryption/decryption process.

06.02 Demonstrate an understanding of the basic functions involved in key management including creation, distribution, verification, revocation, destruction, storage, recovery, and life span of keys.

06.03 Utilize various forms of cryptography, digital certificates, and digital signatures to achieve confidentiality, integrity, authentication, and non-repudiation in an enterprise data communications network.

06.04 Discuss the creation and use of digital certificates and digital signatures to provide authentication of users and verification of data integrity in network communications.

- 06.05 Employ cryptographic algorithms such as DES, RSA, MD5 and DSA.
- 06.06 Identify the strengths and weaknesses of cryptographic algorithms and the effects of key length.
- 06.07 Implement current popular key distribution methods including manual, Kerberos™, and Internet Security Association and Key Management Protocol (ISAKMP).
- 06.08 Utilize application and network-based protocols such as Secure Socket Layer (SSL), Secure HyperText Transfer Protocol (SHTTP), and Internetworking Protocol Security (IPSEC).
- 06.09 Describe the use of hardware components such as smart cards and tokens.
- 07.0 Perform telecommunications and network security activities - The student will be able to:
 - 07.01 Utilize protocol layering models such as the Open Systems Interconnection (OSI) model in analyzing network security threats.
 - 07.02 Evaluate the security implications involved with the various physical media types such as fiber optics, twisted pair, and wireless communications.
 - 07.03 Describe security concerns with using certain network topologies such as star, bus, mesh, and ring.
 - 07.04 Configure authentication protocol services such as RADIUS/TACACS to provide dial-in authentication and security.
 - 07.05 Employ network monitors and packet sniffers to identify security threats.
 - 07.06 Implement security measures using hardware and software such as firewalls, routers, switches, gateways, and proxies.
 - 07.07 Discuss the security vulnerabilities of the Transmission Control Protocol/Internetworking Protocol (TCP/IP) protocol stack.
 - 07.08 Configure Network Layer security protocols such as Internetworking Protocol Security (IPSEC).
 - 07.09 Configure Transport Layer security protocols such as Secure Socket Layer (SSL).
 - 07.10 Utilize Secure Multipurpose Internet Mail Extensions (S/MIME), Secure Socket Layer (SSL) and other Application Layer security protocols.
 - 07.11 Perform connection verification and authentication using Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP).
 - 07.12 Demonstrate an understanding of how wide area network serial line protocols such as Frame relay, X.25, High-level Data Link Control (HDLC), Point-to-Point Protocol (PPP) and Integrated Services Digital Network (ISDN), and Digital Subscriber Line (DSL) work.
 - 07.13 Implement secure data communication techniques such as Virtual Private Networks (VPNs), tunneling, Network Address Translation (NAT), and transmission logging.
 - 07.14 Develop secure e-mail, facsimile, and voice communication procedures to protect against network attacks such as flooding, eavesdropping, sniffing, spamming, etc. and describe appropriate countermeasures.
 - 07.15 Employ alarms and signals to alert network security

administrators of intrusions.

- 08.0 Demonstrate an understanding of Database Management Systems-The student will be able to:
 - 08.01 Compare the major types of databases including relational, flat file, distributed and object-oriented databases.
 - 08.02 Describe the concept of relational database concepts including tables, entity-relationships, queries, and normalization.
 - 08.03 Analyze the various components of a database management system.
 - 08.04 Install and configure database server software from leading vendors.
 - 08.05 Perform database administration tasks using the Structured Query Language (SQL).
 - 08.06 Demonstrate an understanding of transactions processing and concurrency control.
 - 08.07 Perform database backup and recovery operations.
 - 08.08 Employ techniques to ensure database integrity and security.

- 09.0 Perform administrative tasks related to database security-The student will be able to:
 - 09.01 Develop database security guidelines.
 - 09.02 Monitor database security systems.
 - 09.03 Manage web database security.
 - 09.04 Verify security compliance.
 - 09.05 Secure backup processes.
 - 09.06 Verify backup processes.

- 10.0 Demonstrate an understanding of e-commerce-The student will be able to:
 - 10.01 Describe e-commerce and its impact on business and society.
 - 10.02 Differentiate between the various e-commerce business models.
 - 10.03 Describe the development of an e-commerce business plan.
 - 10.04 Discuss e-commerce revenue streams and e-commerce market sectors.
 - 10.05 Develop e-commerce marketing plan.
 - 10.06 Discuss the steps necessary to maintain transaction integrity.
 - 10.07 Identify components and procedures necessary to process credit card transactions.

- 11.0 Perform tasks related to e-commerce security-The student will be able to:
 - 11.01 Manage digital certificates.
 - 11.02 Maintain integrity in transaction storage and reporting systems.
 - 11.03 Protect credit card, personal, banking, and "bill to" and "ship to" information in transaction processes.
 - 11.04 Oversee inventory control.
 - 11.05 Maintain email security related to e-commerce.
 - 11.06 Review third-party transaction processing.
 - 11.07 Assist in evaluating e-commerce platform vulnerabilities.

- 12.0 Perform Web site management activities-The student will be able to:
 - 12.01 Describe the process of obtaining an Internet domain name and mapping it to an Internet Protocol (IP) address.
 - 12.02 Compare features of currently available Web site management

tools.

- 12.03 Configure current Web server software such as Apache Web Server and Microsoft Internet Information Server (IIS).
- 12.04 Use current Web server software to create and maintain a secure Web site.
- 12.05 Use Web site access tracking and analysis tools to evaluate the security of a Web server.
- 13.0 Design and implement physical security measures-The student will be able to:
 - 13.01 Identify the physical threats to an enterprise's resources that include the employees, facilities, data, equipment, support systems, media, and supplies they utilize.
 - 13.02 Diagnose an enterprise's physical vulnerabilities to threats from natural disasters such as fire, flooding, and power loss.
 - 13.03 Specify possible countermeasures to physically protect an enterprise's resources and sensitive information.
 - 13.04 Develop a list of physical facility requirements to secure the premises.
 - 13.05 Evaluate the applicability of technical controls such as smart cards, access logs, and intrusion detection systems.
- 14.0 Perform operations and security management practices-The student will be able to:
 - 14.01 Perform personnel administrative management operations, including specifying job requirements, background checking, job rotation and termination procedures.
 - 14.02 Implement anti-virus solutions on an enterprise-wide basis.
 - 14.03 Perform backups of critical information.
 - 14.04 Protect the privacy of personal data.
 - 14.05 Demonstrate proper handling including marking, handling, storage and destruction of sensitive information and media
 - 14.06 Demonstrate an understanding of different control types. such as directive, preventive, detective, corrective, and recovery controls.
 - 14.07 Determine what resources, including hardware/software, password files, source code, storage and logs, require protection.
 - 14.08 Compare the advantages and disadvantages of internal versus external audits.
 - 14.09 Perform compliance checks on user adherence to security policies.
 - 14.10 Identify different types of monitoring including event, hardware, and illegal software.
 - 14.11 Utilize monitoring tools and techniques such as trend analysis, traffic analysis and reporting mechanisms.
 - 14.12 Implement countermeasures to defend against threats such as fraud, theft, employee sabotage, espionage, terrorism, and hackers.
 - 14.13 Perform penetration testing activities including sniffing, eavesdropping, dumpster diving, and social engineering.
 - 14.14 Understand principles of risk management and asset valuation.
 - 14.15 Monitor server information for defamatory statements and privacy rights infractions.
 - 14.16 Manage software licenses and enforce compliance within the organization.
- 15.0 Employ applications and systems development security techniques-

The student will be able to:

- 15.01 Describe the stages of the system development life cycle.
 - 15.02 Develop and document object-oriented computer programs employing structured programming techniques.
 - 15.03 Analyze the controls that are included within systems and applications software and those used in the development of agents, applets, software, databases, data warehouses and knowledge-based systems.
 - 15.04 Implement features to ensure data and application integrity, security and availability.
 - 15.05 Analyze distributed environment application issues including agents, applets, and objects.
 - 15.06 Analyze local environment application issues including viruses, Trojan horses, logic bombs and worms.
 - 15.07 Analyze key database and data warehousing issues including aggregation, data mining, inference and poly-instantiation
 - 15.08 Develop multilevel security schemes for databases and data warehouses.
 - 15.09 Compare different forms of data/information storage including primary, secondary, real, virtual, random, volatile, and sequential.
 - 15.10 Describe different aspects of application and database security control architectures, including process isolation, hardware segmentation, separation of privilege, layering, abstraction and security kernels.
 - 15.11 Understand the difference between supervisory and user modes of operation.
 - 15.12 Identify various levels of application integrity including network, operating system, database, and file level integrity.
 - 15.13 Define the various types of computer viruses and malicious code and the roles that hackers, crackers, phreaks, and virus writers play in developing and utilizing malicious code.
 - 15.14 Formulate countermeasures to defend against or detect viruses and malicious code.
 - 15.15 Utilize anti-virus software and develop policies to provide enterprise-wide anti-virus protection.
 - 15.16 Employ countermeasures to defend against attacks such as brute force and replay attacks.
- 16.0 Develop business continuity and disaster recovery plans-The student will be able to:
- 16.01 Perform a business impact assessment, including components such as an emergency assessment, specifying business success and critical business functions, establishing priorities, and developing alternative means of accomplishing objectives.
 - 16.02 Specify the necessary capabilities of alternative business sites such as cold, warm, hot and mobile sites to be used in the case of a disaster.
 - 16.03 Develop business continuity, disaster containment, and disaster recovery plans for disasters such as such as floods, fires, power outages, strikes, hardware/software failures, and bombings addressing: protection of physical assets, emergency response, personnel notification, backups and off-site storage, utilities, external communications, and logistics and supplies.
 - 16.04 Describe the process of performing routine scheduled

- maintenance of fire control systems and building utilities such as power, ventilation, and water.
- 16.05 Conduct a business continuity project, including scope and planning.
- 16.06 Develop a training program for personnel regarding business continuity/recovery plans.
- 17.0 Describe ethical issues, pertinent laws, and how to conduct investigations-The student will be able to:
 - 17.01 Understand the major categories and types of laws as to how they relate to E-commerce, including criminal law, civil law and administrative law.
 - 17.02 Develop institutional policies and practices to conform to or supplement existing laws regarding data privacy and intellectual property rights.
 - 17.03 Describe abnormal and suspicious activity as it relates to database and e-commerce security.
 - 17.04 Analyze potential data security threats such as fraud or collusion.
 - 17.05 Develop legal institutional policies and practices to protect against purposeful violations of data integrity.
 - 17.06 Identify the major categories of computer crime and attacks, including military, business, financial, terrorist, grudge and "fun" attacks.
 - 17.07 Develop legal institutional policies and practices to conduct an investigation of purposeful violations of data integrity or existing e-commerce laws, including: the collection and preservation of evidence; confiscation of equipment, software and data; interrogation of suspected violators; and reporting of incidents to the appropriate authorities.
 - 17.08 Discuss major ethical and legal issues related to Internet use.
- 18.0 Perform general organizational computing workplace competencies-The student will be able to:
 - 18.01 Follow oral and written instructions.
 - 18.02 Prepare, outline, and deliver a short oral presentation.
 - 18.03 Prepare visual material to support an oral presentation.
 - 18.04 Participate in group discussions as a member and as a leader.
 - 18.05 Interpret appropriate information from graphics, maps, or signs.
 - 18.06 Demonstrate self-motivation and responsibility to complete an assigned task.
 - 18.07 List the steps in problem solving.
 - 18.08 Identify and discuss issues contained within professional codes of conduct.
 - 18.09 Identify and discuss intellectual property rights and licensing issues.
 - 18.10 Identify potential sources of employee/employer or employee/employee conflict and discuss possible approaches to resolve such disagreements.
 - 18.11 Use appropriate courtesy, manners, and dress in the workplace.
 - 18.12 Apply principles and techniques for being a productive, contributing member of a team.
 - 18.13 Identify and use acceptable strategies for resolving conflict in the workplace.
 - 18.14 Apply principles and techniques for working productively with people of diverse cultures and backgrounds.

- 18.15 Identify techniques for stress management and prevention of job burnout.
- 18.16 Use appropriate communication skills, telephone etiquette, courtesy, and manners when dealing with individuals lacking a technical background.
- 19.0 Perform project planning and management activities-The student will be able to:
 - 19.01 Apply effective time management skills.
 - 19.02 Describe appropriate measures for planning and managing a large project.
 - 19.03 Define an implementation schedule for a large project.
 - 19.04 Describe appropriate measures for planning and implementing corporate-wide upgrade of hardware and software.
 - 19.05 Identify examples of effective end-user training strategies and techniques.
- 20.0 Perform documentation and technical reference activities-The student will be able to:
 - 20.01 Use technical vocabulary appropriately
 - 20.02 Locate information in printed and online technical references
 - 20.03 Prepare documentation to track: physical inventory, regulation and license compliance, hardware and software modifications and upgrades, security breaches and countermeasures, and the current e-commerce security environment
- 21.0 Demonstrate employability skills-The student will be able to:
 - 21.01 Identify sources of employment opportunities.
 - 21.02 Discuss employer expectations regarding attendance, punctuality, initiative, teamwork, etc.
 - 21.03 Discuss employee rights regarding privacy, discrimination, due process, safety, etc.
 - 21.04 Explain the importance of a written job description.
 - 21.05 Identify methods for securing employment references.
 - 21.06 Compose a letter of application and a resume.
 - 21.07 Complete an employment application.
 - 21.08 Classify behaviors considered appropriate or inappropriate in a job interview situation.
 - 21.09 Demonstrate job interview skills.
 - 21.10 Compose a follow-up letter.
 - 21.11 Compose a letter of resignation.
- 22.0 Demonstrate professional development skills-The student will be able to:
 - 22.01 Discover corporate strategies and policies.
 - 22.02 Develop and maintain professional contacts.
 - 22.03 Develop mentor relationships.
 - 22.04 Anticipate future industry trends.
 - 22.05 Describe options for continuing education.
 - 22.06 Read industry journals and magazines.
 - 22.07 Attend seminars, workshops, and tradeshow.