Course Code: Title	CYB101: COMPUTER AND NETWORKING FUNDAMENTALS
Program Number: Name	5911: CYBERSECURITY
Department:	PPP triOS
Academic Year:	2021-2022
Course Description:	This course reviews the essential operating system skills and understanding required for a Cybersecurity professional. More specifically, students learn how to use, configure, upgrade, troubleshoot and maintain computer hardware alongside the Windows family of operating systems, as well as basic configuration of Linux, macOS, and mobile operating systems. At course completion, students will have covered the topics covered on the CompTIA A+ Certification exam.
Total Credits:	4
Hours/Week:	4
Total Hours:	60
Prerequisites:	There are no pre-requisites for this course.
Corequisites:	There are no co-requisites for this course.
Vocational Learning Outcomes (VLO's) addressed in this course: **Please refer to program web page for a complete listing of program outcomes where applicable.**	**5911 - CYBERSECURITY** VLO 1 Develop and implement cyber security solutions to protect network systems and data. VLO 2 Plan and implement security assessment methodologies, vulnerability management strategies and2.incident response procedures to generate and communicate security analysis reports and recommendations to the proper level of the organization. VLO 3 Recommend processes and procedures for maintenance and deployment of cyber security solutions. VLO 10 Maintain ongoing personal and professional development to improve work performance in the field of information technology.
Essential Employability Skills (EES) addressed in this course:	EES 2 Respond to written, spoken, or visual messages in a manner that ensures effective communication. EES 4 Apply a systematic approach to solve problems. EES 5 Use a variety of thinking skills to anticipate and solve problems. EES 6 Locate, select, organize, and document information using appropriate technology and information systems. EES 7 Analyze, evaluate, and apply relevant information from a variety of sources. EES 10 Manage the use of time and other resources to complete projects.
Course Evaluation:	Passing Grade: 50%, D

	A minimum program GPA of 2.0 or higher where program specific standards exist is required for graduation.
Books and Required Resources:	CompTIA A+ Complete Study Guide by Quentin Docter Publisher: Sybex (Wiley) ISBN: 978-1-119-51593-7

Course Outcomes and Learning Objectives:

Course Outcome 1	Learning Objectives for Course Outcome 1
Adopt good technical support skills through a practical understanding of best practices in cybersecurity operational procedures.	OPERATIONAL PROCEDURES 1.1 Exemplify best practices associated with the various types of documentation. 1.2 Implement basic change management best practices. 1.3 Execute basic disaster prevention and recovery methods. 1.4 Examine common safety procedures. 1.5 Explain environmental impacts and appropriate controls. 1.6 Illustrate the process for addressing prohibited content/activity, and privacy, licensing, and policy concepts. 1.7 Exemplify proper communication techniques and professionalism. 1.8 Identify the basics of scripting. 1.9 Apply remote access technologies.

Course Outcome 2	Learning Objectives for Course Outcome 2
Install, configure, maintain, and secure different Windows operating systems and their data.	OPERATING SYSTEMS 2.1 Differentiate between the common operating system types and their purposes. 2.2 Assess the features of Microsoft Windows versions. 2.3 Explain general OS installation considerations and upgrade methods. 2.4 Use appropriate Microsoft command-line tools. 2.5 Use Microsoft operating system features and tools. 2.6 Microsoft Windows Control Panel utilities. 2.7 Outline application installation and configuration concepts. 2.8 Configure Microsoft Windows networking on a client/desktop. 2.9 Utilize features and tools of the macOS and Linux client/desktop operating systems. SECURITY 2.10 Outline the importance of physical security measures. 2.11 Explain logical security concepts. 2.12 Assess wireless security protocols and authentication methods. 2.13 Detect, remove, and prevent malware using appropriate tools and methods. 2.14 Analyze social engineering, threats, and vulnerabilities. 2.15 Differentiate between the basic Microsoft Windows OS security settings. 2.16 Adopt security best practices to secure a workstation 2.17 Implement methods for securing mobile devices.

Course Outcome 3	Learning Objectives for Course Outcome 3
Configure networking protocols and interfaces.	NETWORKING 3.1 Examine TCP and UDP ports, protocols, and their purposes. 3.2 Identify common networking hardware devices. 3.3 Install and configure a basic wired/wireless SOHO network. 3.4 Assess wireless networking protocols. 3.5 Summarize the properties and purposes of services provided by networked hosts. 3.6 Explain common network configuration concepts. 3.7 Compare and contrast Internet connection types, network types, and their features. 3.8 Use appropriate networking tools such as crimper, cable stripper, multimeter, and so on.
Course Outcome 4	**Learning Objectives for Course Outcome 4**
Manage hardware components within PCs and notebooks and mobile devices.	HARDWARE 4.1 Explain basic cable types, features, and their purposes. 4.2 Identify common connector types. 4.3 Select, install, and configure storage devices. 4.4 Explain the purposes and uses of various peripheral types. 4.5 Review power supply types and features. 4.6 Select and configure appropriate components for a custom PC configuration to meet customer specifications or needs. 4.7 Install and configure common devices. 4.8 Configure SOHO multifunction devices/printers and settings. 4.9 Install and maintain various print technologies. 4.10 Install and configure motherboards, CPUs, and add-on cards. 4.11 Install various RAM types. MOBILE DEVICES 4.12 Install and configure laptop hardware and components. 4.13 Install components within the display of a laptop. 4.14 Utilize appropriate laptop features. 4.15 Examine characteristics of various types of other mobile devices. 4.16 Connect and configure accessories and ports of other mobile devices. 4.17 Configure basic mobile device network connectivity and application support. 4.18 Utilize various methods to perform mobile device synchronization.
Course Outcome 5	**Learning Objectives for Course Outcome 5**
Troubleshoot and manage various software and operating system-related issues.	SOFTWARE TROUBLESHOOOTING 5.1 Troubleshoot Microsoft Windows OS problems. 5.2 Troubleshoot and resolve PC security issues. 5.3 Use best practice procedures for malware removal. 5.4 Troubleshoot mobile OS and application issues. 5.5 Troubleshoot mobile OS and application security issues.

Course Outcome 6	Learning Objectives for Course Outcome 6
Troubleshoot common hardware and network problems effectively.	HARDWARE AND NETWORK TROUBLESHOOTING 6.1 Adopt the best practice methodology to resolve problems. 6.2 Troubleshoot common problems related to motherboards, RAM, CPUs, and power. 6.3 Troubleshoot hard drives and RAID arrays. 6.4 Troubleshoot video, projector, and display issues. 6.5 Troubleshoot common mobile device issues while adhering to the appropriate procedures. 6.6 Troubleshoot printers. 6.7 Troubleshoot common wired and wireless network problems.
Course Outcome 7	**Learning Objectives for Course Outcome 7**
Examine cloud computing concepts and configure client-side virtualization.	VIRTUALIZATION AND CLOUD COMPUTING 7.1 Outline cloud computing concepts. 7.2 Set up and configure client-side virtualization.

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Final Exam	60%
Professional Performance	10%
Quizzes	30%

Date: June 30, 2022

Addendum: Please refer to the course outline addendum on the Learning Management System for further information.