

# VALLEY COLLEGE

Student Catalog Addendum

Addendum Date: 2/9/2022

Expected Effective Date: 2/14/2022

Effective Date of Catalog: 1/22/2022

**Valley College has added two 100% Online Diploma programs. Information Technology (IT) and Network Administration and Information Technology (IT) and Security Administration. The revised program outlines and course descriptions are found in this catalog addendum.**

**This information replaced the language in the Student Catalog page: 9 Under the section for Assessments.**

## **Assessment Test for all programs except Practical Nursing and Commercial Driver License (CDL) Class A**

Satisfactory completion of Valley College's Admissions Assessment(s). Valley College uses the Wonderlic Assessment. Valley College also accepts TABE (Tests of Adult Basic Education), ACT or SAT scores. Basic benchmarks scores for the Assessment (based on assessment evaluation tool) for all programs are as follows:

Program	Wonderlic Score	TABE Score	ACT Score	SAT Score
Cybersecurity Diploma, AAS and BS programs	15	10.0	17	1050
All other programs except Practical Nursing and Commercial Driver License (CDL)	10	10.0	17	1050

Admissions Assessment Test process: A designated (trained) Valley College staff /faculty member will administer the admissions assessment test on site or will set up a remote test. Valley College utilizes the online Wonderlic Assessment. A written version of the Wonderlic may be given if it is determined that the prospective student is experiencing computer anxiety or if the Wonderlic web site is not available due to technical reasons. The Wonderlic Admissions Assessment may be taken no more than three times. The prospective student must wait at least fifteen (15) minutes before he or she can retake a Wonderlic assessment.

Applicants who are unable to come to the campus to take their Wonderlic assessment test may take it remotely. The applicant will receive notification via email from Wonderlic when the assessment is set up.

## **This was added to Page 15 under Additional requirements by program:**

### **Additional Requirements – Information Technology (IT) and Security Administration Diploma program**

The Information Technology (IT) and Security Administration program is an advanced diploma program. Students must additional requirements that demonstrate that the student has the basic knowledge either through post-secondary education or prior/current work experience to be successful in this diploma program.

- Prior post-secondary education: The student must either have graduated from Valley College's Information and Network Administration diploma program or the Cybersecurity Associate Degree program or another accredited post-secondary institution with a degree or diploma in Information Technology, Cybersecurity, or a related field.

To demonstrate that the student has met this requirement, Valley College will accept an unofficial transcript at the start of the student's first class. However, the student **must provide** the college with **an official transcript** showing the student has completed the program by the student's midpoint in the program. Failing to provide the college with an official transcript will result in termination from the program.

If the applicant does not have the required post-secondary education requirement, the applicant must meet the following requirements:

- Have a minimum of 2 years of professional experience in the Cybersecurity and/or Information Technology Field; and
- Holds an industry recognized certification in Networking or an equal-level Cybersecurity and/or Information Technology nationally recognized professional certification.

Valley College will accept the student’s resume demonstrating their professional and educational credentials and a copy of their certification credential(s) as proof of meeting these requirements. The resume and certification credentials will be reviewed by Valley College. If the College determines that the student does not meet these requirements, the student will not be able to continue in the program. The student must provide the information to the College by the first day of class and the determination will be made by the end of the start period (12 consecutive days after the first day of class).

On Page 73, the two new programs were added under Schedules:

### **Programs Delivered Online – Schedules**

Online programs are offered and administered through the main campus, Valley College – Martinsburg. Valley College – Martinsburg is a member of the National Council for State Authorization Reciprocity Association (SARA) and is authorized to deliver distance education to students who reside in states that are also members of NC-SARA. While a class is in session, students may access their classes 24/7, unless there is a scheduled or unscheduled maintenance issue with Moodlerooms. Notices for scheduled maintenance are posted to allow students to adjust their schedules accordingly.

<b>Start Date</b>	<b>MFOBC and MAA Projected completion date</b>	<b>ITNA &amp; ITNS Projected completion date</b>
1/3/2022	9/1/2022	<b>N/A</b>
1/24/2022	9/22/2022	<b>N/A</b>
2/14/2022	10/13/2022	9/22/2022
3/7/2022	11/3/2022	10/13/2022
4/4/2022	11/30/2022	11/3/2022
4/25/2022	12/22/2022	11/30/2022
5/16/2022	1/26/2023	12/22/2022
6/6/2022	2/16/2023	1/26/2023
7/5/2022	3/9/2023	2/16/2023
7/25/2022	3/30/2023	3/9/2023
8/15/2022	4/20/2023	3/30/2023
9/6/2022	5/11/2023	4/20/2023
9/26/2022	6/1/2023	5/11/2023
10/17/2022	6/22/2023	6/1/2023
11/7/2022	7/20/2023	6/22/2023
12/5/2022	8/10/2023	7/20/2023

In the Program Descriptions and Outlines section, On Page 74, the two new programs were added to the Program Summary Chart.

### Program Summary Chart

For regular attendance, standard completion times are expressed in full weeks/months. The week schedules are for instructional/contact hours. The range in estimated month schedules includes holidays and breaks and vary depending on time of year of the start date.

Campus and Program Name	Credential	Delivered	Credits	Hrs/Wk	Total Hrs	Weeks	Months
M Business Administration	Bachelor (BS)	Online	125	20.0	2400	114	31
M Cybersecurity	Bachelor (BS)	Online	126	20.0	2400	120	31
M Health Services Administration	Bachelor (BS)	Online	126	20.0	2460	123	32
M Business Administration	Associate (AAB)	Online	61	20.0	1200	61	16
M Cybersecurity	Associate (AAS)	Online	65	20.0	1200	60	16
M Health Services Administration	Associate (AAB)	Online	63	20.0	1260	63	17
M Information Technology (IT) and Network Administration	Diploma	Online	30	20.0	600	30	8
M Information Technology (IT) and Security Administration	Diploma	Online	30	20.0	600	30	8
M Medical Administrative Assistant	Diploma	Online	30	20.0	660	33	9
B C M Medical Clinical Assistant	Diploma	Blended	38	20.0	825	39	10
M Medical Front Office, Billing and Coding	Diploma	Online	30	20.0	660	33	9
C F Practical Nursing	Diploma	Blended	36	20.0	924	39	10
C Veterinary Assistant	Diploma	Blended	30	20.0	600	30	8
C Veterinary Technician	Associate (AAS)	Blended	65	20.0	1560	74	19
C Commercial Driver License (CDL) – Class A	Certificate	On Campus	0	32.0	160	5	2

Total hours do not reflect out-of-class assignments.

Key: B = Beckley Campus, M = Martinsburg Campus, C = Cleveland Campus, and F = Fairlawn Satellite (Learning Center)

This information was added to page 103-105

### Information Technology (IT) and Network Administration – DE Diploma

<https://valley.edu/programs/cybersecurity-training/>

Credential: Diploma

Delivered online and approved to be administrated through Valley College - Martinsburg (WV)

#### Program Description

The Information Technology (IT) and Network Administration (ITNA) Diploma program is designed to equip graduates with the skills to create, administer and secure various types of networking structures. Students will learn to identify and assess the essential components of various types of networking systems and supporting hardware. This program will enable students to also analyze the capabilities and needs of multiple types of operating systems and the corresponding security needs of computer and network systems in both personal and business settings.

The ITNA program will also provide instruction in Network Application Support, IT Help Desk principles, protocols, and problem solving, and principles of customer service. Further, students will also learn how to synthesize networking design with security protocols and procedures and will also be introduced to a series of concepts to pro-actively and re-actively respond to internal and external hacking activities. Through an integrated curriculum that includes hands on assignments/activities/projects and computer-mediated discussions, students will demonstrate mastery of the objectives which will be measured by graded assignments, discussion responses, quizzes, tests, and rubric-based assessment of projects. The skills and concepts learned can transfer to the work environment. The ITNA program prepares students for entry-level positions in the Information Technology and Cybersecurity industry ranging from IT positions to Help Desk to Network Specialist.

ITNA students receive a license to use Practice Labs. Due to software license restrictions, the plan is only valid for current students. The College must deactivate the student's access to Practice Labs when he or she graduates or withdraws from the program. The student must abide by additional requirements as described in the Student Code of Conduct to be able to use Practice Labs. Finally, students will also gain access to the Comp-TIA's Cert-Master Learning Management System where they will have an opportunity to compete the requirements associated with the Comp-TIA Network + Certification at the conclusion of the program.

#### Program/Student Learning Outcomes

1. Explain and demonstrate how the basic components, features, and technologies needed to set up and support a computer network.
2. Execute troubleshooting techniques that can be used to solve computer, hardware, and network problems for individual users and/or organizations.
3. Demonstrate fundamental knowledge of TCP/IP, its layers, and common protocols.
4. Explain and demonstrate an understanding of network protocols, their function, and their role in secure network communications.
5. Explain routing characteristics, commands, and protocols and demonstrate the ability to complete as part of networking setup and ongoing support.
6. Demonstrate the ability to identify and assess the functions of an operating system and secure configuration of the operating system and hardware.
7. Explain and execute the steps to assess, secure, monitor, and defend a network.
8. Execute the required steps and key considerations to install, operate, and troubleshoot network equipment.
9. Evaluate the composition of a program and how to modify the program using problem-solving methodologies.
10. Identify and demonstrate an understanding of the characteristics of IPv4 and IPv6 addressing and routing.
11. Demonstrate the ability to explain and execute internal and external intrusion risks and how to effectively use detection technologies and prevention systems.

### Program Outline

The schedules will vary. The student receives their initial rotation schedule (course schedule) during the admissions process.

Tier	Course Number	Course Name	Semester Credits	Contact Hours	Lecture Hours	Lab Hours
1	CSY105	Introduction to Networking	3.0	60	30	30
1	CSY110	Networking Hardware	3.0	60	30	30
1	CSY115	Routing & Security Protocols	3.0	60	30	30
2	CSY125	Operating Systems	3.0	60	30	30
2	CSY130	Network Security	3.0	60	30	30
2	CSY200	Introduction to Programming	3.0	60	30	30
3	CSY140	Network & Security Fundamentals	3.0	60	30	30
3	CSY120	Network Application Support	3.0	60	30	30
3	CSY330	IT Help Desk	3.0	60	30	30
3	CSY205	Ethical Hacking and System Security	3.0	60	30	30
Totals			30.0	600	300	300

Additional Out-of-Class hours should be expected to include assignments and reading.

### Career Opportunities

#### CIP CODE: 11.1006

This program is intended for persons who desire a concentrated program in the Information Technology/ Cybersecurity industry and who wish to pursue a career. Examples of positions graduates may be qualified for entry-level positions and/or may find advancement opportunities into include, but are not limited to:

- \*Computer Specialist
- \*Computer Support Specialist
- \*Desktop Support Technician
- \*Help Desk Specialist
- \*Information Technology Specialist
- \*Support Specialist

Valley College is a proud partner of CompTIA. The Cybersecurity AAS program will help prepare you for the: Networking + certification exam

Please go to the CompTIA web site <https://certification.comptia.org/certifications> for more information regarding the requirements for each of these exams or contact your Career Service Advisor.

## Information Technology (IT) and Security Administration – (ITSA) DE Diploma

<https://valley.edu/programs/cybersecurity-training/>

Credential: Diploma

Delivered online and approved to be administrated through Valley College - Martinsburg (WV)

### Program Description

The Information Technology (IT) and Security Administration Diploma (ITSA) program is designed to equip graduates with the skills to create, administer and secure various types of computers, technological devices, and networks. Students will learn to analyze and evaluate the essential components of various types of hardware, devices, systems and supporting hardware. This program will enable students to analyze and evaluate the capabilities and needs of multiple types of operating systems and the corresponding security needs of computer and network systems in both personal and business settings.

The ITSA program will also provide instruction in Information Security, Secure Wireless Networking, Security Countermeasures, and Systems Analysis and Design. All courses will focus, protocols, and problem solving, and principles of customer service. Further, students will also learn how to synthesize networking design with security protocols and procedures and will also be introduced to a series of concepts to pro-actively and re-actively respond to internal and external hacking activities.

Through an integrated curriculum that includes hands on assignments/activities/projects and computer-mediated discussions, students will demonstrate mastery of the objectives which will be measured by graded assignments, discussion responses, quizzes, tests, and rubric-based assessment of projects. The skills and concepts learned can transfer to the work environment. The ITSA program prepares students for entry-level positions in the Information Technology and Cybersecurity industry ranging from IT positions to Help Desk to Security Specialist, and Systems Analysis and Design.

ITSA students receive a license to use Practice Labs. Due to software license restrictions, the plan is only valid for current students. The College must deactivate the student's access to Practice Labs when he or she graduates or withdraws from the program. The student must abide by additional requirements as described in the Student Code of Conduct to be able to use Practice Labs. Finally, students will also gain access to the Comp-TIA's Cert-Master Learning Management System where they will have an opportunity to compete the requirements associated with the Comp-TIA Security + Certification at the conclusion of the program.

### Program/Student Learning Outcomes

1. Explain and demonstrate how to setup and support computer networks and the methodology to troubleshoot and manage network security.
2. Execute troubleshooting techniques and processes that can be used to identify and solve internal and external security risks for individual users and/or organizations.
3. Conduct risk-management activities to pro-actively monitor, test, analyze, and evaluate security risks.
4. Evaluate the advantages, disadvantages and corresponding concerns and features of securing a wireless infrastructure.
5. Determine the most effective form of data acquisition, supporting resources and tools, when investigating a data security breach.
6. Demonstrate the ability to assess and analyze the specifics of an intrusion and how to execute a countermeasure to secure a network or device.
7. Explain and execute the steps associated with building a database along with a data recovery process and security services to protect the data.
8. Create a security model that accounts for strategic governance policies and processes, regulatory standards, and compliance requirements.
9. Develop the ability to explain and execute various techniques for measuring, managing, and planning system performance, while accounting equally for system security.
10. Describe and demonstrate the ability to read, write, and interpret basic code.
11. Develop the ability to write, run, and debug, and secure a program.

### Program Outline

The schedules will vary. The student receives their initial rotation schedule (course schedule) during the admissions process.

Tier	Course Number	Course Name	Semester Credits	Contact Hours	Lecture Hours	Lab Hours
1	CSY145	Advanced Network & Security Fundamentals	3.0	60	30	30
1	CSY215	Information Security	3.0	60	30	30
1	CSY220	Secure Wireless Networks	3.0	60	30	30
2	CSY320	Digital Forensics	3.0	60	30	30
2	CSY340	Security Countermeasures	3.0	60	30	30
2	CSY350	Database Management	3.0	60	30	30
3	CSY360	Introduction to Cyber Crimes and Homeland Security	3.0	60	30	30
3	CSY400	System Analysis and Design	3.0	60	30	30
3	CSY420	Cyber Law	3.0	60	30	30
3	CSY430	Introduction to Scripting	3.0	60	30	30
Totals			30.0	600	300	300

Additional Out-of-Class hours should be expected to include assignments and reading.

### Career Opportunities

#### CIP CODE: 11.1006

This program is intended for persons who desire a concentrated program in the Information Technology/ Cybersecurity industry and who wish to pursue a career. Examples of positions graduates may be qualified for entry-level positions and/or may find advancement opportunities into include, but are not limited to:

- \*Computer Technician
- \*Information Assurance Security Specialist
- \*Information Systems Security Specialist
- \*IT Security Specialist
- \*Network Security Consultant
- \*Technical Support Specialist

Valley College is a proud partner of CompTIA. The Cybersecurity AAS program will help prepare you for the: Security + certification exam

Please go to the CompTIA web site <https://certification.comptia.org/certifications> for more information regarding the requirements for each of these exams or contact your Career Service Advisor.

## Course Descriptions

### **CSY105 - Introduction to Networking**

#### **3.0 Semester Credits**

Introduction to Networking offers an introduction to computer networks and related technologies. Students will develop a solid foundation in basic networking fundamentals, including design, configuration, backup, and recovery. Students will also be introduced to additional topics that revolve around LANs, VLANs, Wireless Networks, TCP/IP, and Ethernet. In addition, students will also be presented with a series of practices that they can use to pro-actively protect networks from internal and external intrusion

Students will also gain an understanding of protocols, topologies, hardware, and troubleshooting. Finally, students will apply the concepts presented in this course to a host of activities and case projects that explore various networking activities that cybersecurity professionals face in industry settings.

### **CSY110 --Networking Hardware**

#### **3.0 Semester Credits**

Networking Hardware will introduce students to a host of fundamental topics. Students will be introduced to networking fundamentals and additional supporting topics that include the OSI Reference Model and TCP/IP. Students will also be exposed to topics that include network components, Ethernet, IPv4, IPv6, and Routing IP Packets. Building on these subjects, students will then gain an understanding of WAN's, Wireless LAN's, Network Optimization, Management, and Security.

As an element of these of these activities, students will also work with the different network topologies, hubs, bridges, switches, routers, and modems will all be explored. Students will also learn about Ethernet technology and network design. Finally, students will apply these concepts to a host of practical based activities to help them understand how to effectively and proactively troubleshoot and protect networks from internal and external intrusions.

### **CSY115 - Routing & Security Protocols**

#### **3.0 Semester Credits**

Routing & Security Protocols offers an introduction to the different levels of network protocols. The course will cover topics such as: IP addressing, IP packet structures, IP address auto-configuration, name resolution, and interoperation.

### **CSY125 - Operating Systems**

#### **3.0 Semester Credits**

Operating Systems is designed to offer students an introduction to computer operating systems. Students will learn about the different theories, concepts, and technologies that go into the functionality of the major operating systems. Building on the theories and concepts of each major operating system, students will be placed into a series of labs that will require them to install and manage various systems. Further, students will also troubleshoot various operating system issues through a host of simulated scenarios that will enable the student to create problem-solving strategies for protecting each type of operating system.

### **CSY130 - Network Security**

#### **3.0 Semester Credits**

Network Security provides an introduction to network security and cryptography. Students will learn about core computer system security, OS hardening and virtualization, application security, network design elements and corresponding threats, security network media, encryption levels, hardware and software components, and forensic techniques.

Troubleshooting techniques will also be emphasized as an element of teach topic. Finally, students will be presented with an opportunity to practically apply the concepts and theories throughout the course with a host of labs and simulations specific to key course content.

### **CSY140 - Network & Security Fundamentals**

#### **3.0 Semester Credits**

Network & Security Fundamentals will cover key network fundamentals, such as LANS, WANs, Ipv4 addressing and sub-netting, and configuring and verifying host connectivity. Students will also learn the processes involved in network analysis and troubleshooting. Students will develop problem-solving skills and additional means to proactively configure, secure, and consistently analyze each of these systems through a variety of labs and simulations.

### **CSY145 - Advanced Network & Security Fundamentals**

#### **3.0 Semester Credits**

##### **Pre-requisite: CSY140**

Advanced Network & Security Fundamentals will cover key network fundamentals, such as LANS, WANs, Ipv4 addressing and sub-netting, and configuring and verifying host connectivity. Students will also learn the processes involved in network analysis and troubleshooting. Students will build on previous coursework with advanced work specific to proactively assess and analyze networks and systems in order to configure, secure, and consistently analyze each of these systems through a variety of labs and simulations.

### **CSY200 -Introduction to Programming**

#### **3.0 Semester Credits**

Introduction to Programming provides an introduction to fundamental programming skills. Students will learn to follow the problem-solving process when coding. Students will be introduced to concepts that include control statements, strings, lists, dictionaries, and how to design using functions. In addition, students will also be introduced to simple graphics, image processing, and instructed on how to design with classes. Finally,

students will also be introduced to graphical user interfaces, multithreading, client/server programming, and the principles of searching, sorting, and complexity analysis.

### **CSY205 - Ethical Hacking and System Security**

#### **3.0 Semester Credits**

Ethical Hacking and System Security provides students with a balanced approach of ethical hacking procedures and guidelines and the corresponding practical skills that will enable students to utilize tools and resources to protect and secure their system. Students will be presented with essential concepts that illustrate ethical and hacking principles. Building on these concepts and principles, students will then be introduced to countermeasures that can be taken from both a pre-emptive perspective and in response to system attacks. Ultimately, students will use this balanced approach to minimize the risk and impact of cyber-attacks from both potential internal and external sources.

### **CSY215- Information Security**

#### **3.0 Semester Credits**

Information Security is designed to offer students a broad perspective of the entire field of information security. Students will learn key information security terms, the history of information security, and an overview of how to properly manage information security.

### **CSY220 - Secure Wireless Networks**

#### **3.0 Semester Credits**

Secure Wireless Networks provides an introduction to wireless data communications. Students will learn the fundamentals of wireless communication, including protocols, transmissions, and standards that make the communication possible and secure. Technologies for wireless network capabilities will also be discussed.

### **CSY320 - Digital Forensics**

#### **3.0 Semester Credits**

CSY320 will provide students with a combination of theoretical concepts, processes and techniques to perform computer and digital based forensic investigation and analysis. The student will gain an understanding of the techniques and practices associated with gathering, preparing, and analyzing information and digital artifacts in an effort to perform root cause analysis in support of breach investigation and incident response. In addition, students will be introduced to cyber-crime investigation involving computers and other technological devices and resources.

Students will apply these concepts, tools, and techniques through a host of hands-on projects. Throughout the course, students will learn how to effectively and efficiently illustrate the process, procedures, ethical considerations, legal/compliance requirements, and reporting associated with the various computer forensic investigations presented in this course.

### **CSY330 - IT Help Desk**

#### **3.0 Semester Credits**

CSY330 will prepare students for working with customers in the role of an IT Help Desk professional. Students will gain important customer service skills that focus on active listening, written and verbal communication, problem-solving, decision-making, managing stress, time management, and teamwork.

Throughout the course, students will learn how to relate these customer service skills to the current and emerging trends of the information technology industry, which includes supporting; personal computers/laptops, operating systems, cloud and mobile computing, virtualization, network communication setup and troubleshooting, as well as Linux and Apple Mac OS. Students will apply the skills they have learned in this class to complete case studies, projects, and practical on-the-job activities. Finally, students will need to utilize these skills to create solutions in an IT Help Desk environment.

### **CSY340 - Security Countermeasures**

#### **3.0 Semester Credits**

This course will provide students with the fundamental concepts associated with intrusion detection, prevention concepts for various systems, and the corresponding skills associated with developing a security policy. In coordination with the security policy, students will also learn how to implement the security policy by first establishing Network Address Translation and then continuing that process by learning concepts and practices associated with packet filtering, installing proxy servers, firewalls, and Virtual Private Networks (VPN). In addition, students will also be introduced to the concepts associated with cryptography, perimeter defense and security counter-measures in networks

### **CSY350 - Database Management**

#### **3.0 Semester Credits**

This course introduces students to the knowledge and skills that Cybersecurity professionals need as it pertains to database design, data integrity, database internals, and data security enabling the student to cultivate an in demand hard IT skill. Students will learn the concepts and techniques that correspond with SQL syntax and further, includes additional focus on core topics that include E-R diagrams, normalization, database administration, NoSQL, database connectivity and management. Building on these concepts, students will also learn concepts that relate to distributed databases, data warehouses, stored procedures, triggers, data macros, and Web-based applications.

Students will apply the concepts and techniques presented in this course to various types of case studies and organizational examples presented in the course. The labs will enable the students to demonstrate critical thinking skills and the application of the concepts presented in each chapter in order to create a solution for various sorts of security and intrusion threats to multiple forms of databases.

### **CSY400 - System Analysis and Design**

#### **3.0 Semester Credits**

CSY400 presents students with a thorough understanding of systems analysis and design. This course will provide essential concepts and techniques that will enable the students to learn how to analyze business needs and then, manage systems, projects, utilize various modeling plans,

and design data and the overall system architecture. Further, students will also learn to manage the implementation of a new system in a business environment and then, create and execute the steps associated with managing systems support and security efforts for the organization.

Students will have an opportunity to apply these concepts to a series of real-world examples and case studies throughout the course. These examples and case studies will require the student to apply critical thinking skills to assess, analyze, and evaluate the overall situation. Based on the evaluation of these situations, students will be asked to apply the concepts and techniques introduced in this course to create a solution that meets the needs and requirements of the organization.

### **CSY420 - Cyber Law**

#### **3.0 Semester Credits**

Cyber Law presents students with the complex legal issues that are related to today's business environment and more specifically, the technology based elements of business today. Students will be presented with essential topics and concepts that deal with; privacy, patents, antitrust, copyright, trademarks, domain names, biotechnology, tort liability, contracts, and conduct.

Students will also be presented with a series of historical and landmark cases and judicial decisions that will enable the student to associate the topics and concepts with practical real-life examples. Students will then have the opportunity to apply the topics and concepts presented in this course, along with the cases and decisions presented in the text, through various exercises and case studies in order to understand the impact of practices on potential legal issues and considerations that are related to technology and corresponding business practices.

### **CSY430 - Introduction to Scripting**

#### **3.0 Semester Credits**

This course presents students with a comprehensive understanding of the concepts and principles associated with programming and scripting. This course will provide students with an opportunity to learn the fundamental steps in interacting with software to create the scripts. Course concepts are introduced using a spiral model focused on Python and additional details and background for these constructs are introduced. Students will also be exposed to important computer science concepts when the concepts are needed to solve a problem.

Students are provided the opportunity to apply the concepts and principles presented, with a series of hands-on activities where they develop their own scripts. Students create a computer game based on the concepts presented in this class. These activities provide students with the foundation of knowledge and practical skills that will prepare them for the challenges they will face as a Cybersecurity professional.