COURSE OUTLINE: CYB301 - SECURITY/DEFENSE/RES

Prepared: IT Studies
Approved: Corey Meunier, Chair, Technology and Skilled Trades

Course Code: Title	CYB301: SECURITY, DEFENSE AND RESPONSE
Program Number: Name	5911: CYBERSECURITY
Department:	PPP triOS
Academic Year:	2021-2022
Course Description:	This course covers IT security defense and response in the Canadian and Ontario regulatory environments. This course covers the procedures used to implement and configure security within an enterprise environment, as well as respond to security incidents. Focus will be placed on tools that can be used to secure access to data and mitigate security breaches.
Total Credits:	5
Hours/Week:	5
Total Hours:	75
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 5 Comply with existing industry policies, regulations, and ethics for information systems and information technology security solutions to ensure industry expectations and standards are met or exceeded. VLO 6 Analyze security risks to organizations and business processes to mitigate risk in compliance with industry standards. VLO 8 Implement and conduct penetration testing to identify and exploit an organization's network system vulnerability. VLO 9 Perform various types of cyber analysis to detect actual security incidents and suggest solutions.
Essential Employability Skills (EES) addressed in this course:	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 9 Interact with others in groups or teams that contribute to effective working relationships and the achievement of goals. 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.

Other Course Evaluation & Assessment Requirements:

Definition Grade Point Equivalent A+ 90 - 100% 4.00
A 80 - 89% 4.00
B 70 - 79% 3.00
C 60 - 69% 2.00
D 50 - 59% 1.00
F(Fail) below 50% 0.00

Books and Required Resources:

CompTIA Security+ Study Guide by Emmett Dulaney and Chuck Easttom
Publisher: Sybex (Wiley)
ISBN: 978-1-119-41687-6

CompTIA CySA+ Study Guide by Mike Chapple
Publisher: Sybex (Wiley)
ISBN: 978-1-119-68405-3

Course Outcomes and Learning Objectives:

Course Outcome 1	**Learning Objectives for Course Outcome 1**
Analyze indicators and various threats, attacks, and vulnerabilities and explain the impact associated with each.	THREATS, ATTACKS, AND VULNERABILITIES 1.1 Analyze indicators of compromise and determine the type of malware for various scenarios. 1.2 Assess the different types of attacks. 1.4 Examine penetration testing concepts. 1.5 Review vulnerability scanning concepts. 1.6 Explain the impact associated with types of vulnerabilities.
Course Outcome 2	**Learning Objectives for Course Outcome 2**
Install and configure network components and implement secure protocols.	TECHNOLOGIES AND TOOLS 2.1 Install and configure network components, both hardware- and software-based, to support organizational security. 2.2 Use appropriate software tools to assess the security posture of an organization for various scenarios. 2.3 Troubleshoot common security issues. 2.4 Analyze and interpret output from security technologies. 2.5 Deploy mobile devices securely. 2.6 Implement secure protocols.
Course Outcome 3	**Learning Objectives for Course Outcome 3**
Evaluate the importance of physical controls and various frameworks for risk mitigation and secure systems design.	ARCHITECTURE AND DESIGN 3.1 Explain use cases and purpose for frameworks, best practices, and secure configuration guides. 3.2 Implement secure network architecture concepts for various scenarios. 3.3 Implement secure systems design. 3.4 Explain the importance of secure staging deployment concepts. 3.5 Examine the security implications of embedded systems. 3.6 Review secure application development and deployment concepts. 3.7 Analyze cloud and virtualization concepts. 3.8 Explain how resiliency and automation strategies reduce

	risk. 3.9 Assess the importance of physical security controls.
Course Outcome 4	**Learning Objectives for Course Outcome 4**
Analyze the differences in various identity and access management concepts and controls, and install and configure identity and access services.	IDENTITY AND ACCESS MANAGEMENT 4.1 Compare and contrast identity and access management concepts. 4.2 Install and configure identity and access services. 4.3 Implement identity and access management controls. 4.4 Examine common account management practices.
Course Outcome 5	**Learning Objectives for Course Outcome 5**
Adopt risk management processes and concepts.	RISK MANAGEMENT 5.1 Explain the importance of policies, plans and procedures related to organizational security. 5.2 Review business impact analysis concepts. 5.3 Explain risk management processes and concepts. 5.4 Specify incident response procedures. 5.5 Examine basic concepts of forensics. 5.6 Explain disaster recovery and continuity of operation concepts. 5.7 Outline various types of controls. 5.8 Execute data security and privacy practices.
Course Outcome 6	**Learning Objectives for Course Outcome 6**
Assess the basic concepts of cryptography and implement public key infrastructure in a scenario.	CRYPTOGRAPHY AND PKI 6.1 Review basic concepts of cryptography. 6.2 Explain cryptography algorithms and their basic characteristics. 6.3 Install and configure wireless security settings. 6.4 Implement public key infrastructure.
Course Outcome 7	**Learning Objectives for Course Outcome 7**
Recommend appropriate responses to threats after implementing various reconnaissance technique and analyzing the results.	THREAT MANAGEMENT 7.1 Perform environmental reconnaissance techniques using appropriate tools and processes. 7.2 Analyze the results of a network reconnaissance. 7.3 Given a network-based threat, implement or recommend the appropriate response and countermeasure. 7.4 Explain the purpose of practices used to secure a corporate environment.
Course Outcome 8	**Learning Objectives for Course Outcome 8**
Perform vulnerability management processes.	VULNERABILITY MANAGEMENT 8.1 Given a scenario, implement an information security vulnerability management process. 8.2 Analyze the output resulting from a vulnerability scan in various scenarios.
Course Outcome 9	**Learning Objectives for Course Outcome 9**
Recommend the best approach and response to a cyber incident.	CYBER INCIDENT RESPONSE 9.1 Distinguish threat data or behavior to determine the impact of a cyber incident.

	9.2 Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation. 9.3 Explain the importance of communication during the incident response process. 9.4 Analyze common symptoms to select the best course of action to support incident response. 9.5 Review the incident recovery and post-incident response process.
Course Outcome 10	**Learning Objectives for Course Outcome 10**
Outline the relationship between frameworks, policies, controls, and procedures and adopt application security best practices.	SECURITY ARCHITECTURE AND TOOL SETS 10.1 Explain the relationship between frameworks, common policies, controls, and procedures. 10.2 Use data to recommend remediation of security issues related to identity and access management. 10.3 Review security architecture and make recommendations to implement compensating controls. 10.4 Adopt application security best practices while participating in the Software Development Life Cycle (SDLC). 10.5 Evaluate the general purpose and reasons for using various cybersecurity tools and technologies.

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Final Exam	60%
Lab Work and Assignments	30%
Professional Performance	10%

Date:

June 30, 2022

Addendum:

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