Course Code: Title	CYB102: WINDOWS ADMINISTRATION & POWERSHELL SCRI
Program Number: Name	2198: CYBERSECURITY 5911: CYBERSECURITY
Department:	PPP triOS
Academic Year:	2023-2024
Course Description:	Students will apply hands-on skills in cyber-security management of Cloud-based and on-premises Windows network environments. The course utilizes defense strategies through an understanding of system and file permissions, password and account security, group policy, registry, encryption, and firewall management. Cyber Security best practices using the zero trust framework model will be implemented to secure and protect data from unauthorized users and cyber-criminals.
Total Credits:	4
Hours/Week:	4
Total Hours:	56
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.**	**2198 - 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 and 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 VLO 7 Plan and conduct disaster recovery, forensic investigations and incident responses to support Business Continuity of an organization 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 **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.

SAULT COLLEGE | 443 NORTHERN AVENUE | SAULT STE. MARIE, ON P6B 4J3, CANADA | 705-759-2554

	VLO 3	Recommend processes and procedures for maintenance and deployment of cyber security solutions.
	VLO 7	Plan and conduct disaster recovery, forensic investigations and incident responses to support Business Continuity of an organization.
	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 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:	A+ = 90-100% A = 80-89% B = 70-79% C = 60-69% D = 50-59% F < 50%	

Students are expected to be present to write all tests in class, unless otherwise specified. If a student is unable to write a test due to illness or a legitimate emergency, that student must contact the professor prior to class and provide reasoning. Should the student fail to contact the professor, the student shall receive a grade of zero on the test.

If a student is not present 10 minutes after the test begins, the student will be considered absent and will not be given the privilege of writing the test.
Students exhibiting academic dishonesty during a test will receive an automatic zero. Please refer to the College Academic Dishonesty Policy for further information.

In order to qualify to write a missed test, the student shall have:
a.) attended at least 75% of the classes to-date.
b.) provide the professor an acceptable explanation for his/her absence.
c.) be granted permission by the professor.

NOTE: The missed test that has met the above criteria will be an end-of-semester test.
Labs / assignments are due on the due-date indicated by the professor. Notice by the professor will be written on the labs / assignments and verbally announced in the class. Labs and assignments that are deemed late will have the following penalty: 1 day late - 10% reduction, 2 days late, 20% reduction, 3 days late, 30% reduction. After 3 days, no late assignments and labs will be accepted. It is the responsibility of the student who has missed a class to contact the professor immediately to obtain the lab / assignment. Students are responsible for doing their own work. Labs / assignments that are handed in and are deemed identical or near

identical in content may constitute academic dishonesty and result in a zero grade.

Students are expected to be present to write in-classroom quizzes. There are no make-up options for missed in-class quizzes.

Students have the right to learn in an environment that is distraction-free, therefore, everyone is expected to arrive on-time in class. Should lectures become distracted due to students walking in late, the professor may deny entry until the 1st break period, which is 50 minutes into the class or until that component of the lecture is complete.

The total overall average of test scores combined must be 50% or higher in order to qualify to pass this course. In addition, combined tests, Labs / Assignments total grade must be 50% or higher.

Course Outcomes and Learning Objectives:

Course Outcome 1	Learning Objectives for Course Outcome 1
Introduction to Microsoft Azure in the Cloud	1.1 Discuss the customer shift from on-premises to cloud-based server solutions 1.2 Contrast Microsoft Azure Active Directory to on-premises Active Directory 1.3 Compare network solution pricing between Microsoft Azure vs Windows Server on-premises 1.4 Identify key components required to configure a Windows Server in the cloud 1.5 Identify then utilize key management menus for Microsoft Azure Active Directory
Course Outcome 2	**Learning Objectives for Course Outcome 2**
Administer a Microsoft Azure Active Directory Server	2.1 Explain the zero-trust framework 2.2 Create user accounts 2.3 Create groups 2.4 Allocate users to specific groups 2.5 Create Folders and Files 2.6 Apply security to folders and files specific to groups and users needs 2.7 Apply auditing to folder and file access and user account logins
Course Outcome 3	**Learning Objectives for Course Outcome 3**
Secure, monitor then test the Cloud Server	3.1 Explain then apply Firewall rules to the network 3.2 Apply Policies to secure folder, file and network access 3.3 Monitor cloud server activities using built-in and 3rd party tools 3.4 Apply hands-on client activities to test cloud network
Course Outcome 4	**Learning Objectives for Course Outcome 4**
Install and configure a Windows on-premisis Network Server	4.1 Download Windows Server source files and license key from the Microsoft Academic Alliance site 4.2 Create a Windows Server Virtual image 4.3 Install a Windows Server on a Virtual Machine 4.4 Login to Windows Server and create a backup Administrator account 4.5 Configure TCP/IP to access the network and Internet

		4.6 Lockdown Windows Server using a Firewall, Anti-Virus and Service Pack updates 4.7 Install and configure a DNS Server 4.8 Promote Windows Server to a Domain Controller in an Active Directory model
	Course Outcome 5	**Learning Objectives for Course Outcome 5**
	Administer a Windows Server (Users and Groups)	5.1 Explore Administrative Tools 5.2 Work with `Active Directory Users and Computers` tool 5.3 Contrast Network User Accounts and Group Types 5.4 Create User Accounts and Domain Local Groups using both the admin menu and powershell command line 5.5 Add Users to specific groups
	Course Outcome 6	**Learning Objectives for Course Outcome 6**
	Administer and Secure Windows Server (Shares, Folders and Files)	6.1 Explore Share Level Permissions 6.2 Identify the various Security settings 6.3 Apply Folder and File Level Security 6.4 Contrast Share level vs Folder / File level Security 6.5 Apply and test Shares / Folders and File Permissions in an NTFS-based environment using hands-on business lab examples 6.6 Use Windows 10 client to test Windows Server Share / Folder / File level security
	Course Outcome 7	**Learning Objectives for Course Outcome 7**
	Install and Configure Web Services	7.1 Install and configure an IIS Web Server 7.2 Install and configure an FTP Server 7.3 Create a Website for testing purposes 7.4 Apply and test various security settings to your website using basic, windows and reverse encryption authentication processes 7.5 View then analyse Web and FTP Server weblogs 7.6 Create a custom error-reporting webpage 7.7 Explain the role of Certificate Services 7.8 Analyze Web Certificates
	Course Outcome 8	**Learning Objectives for Course Outcome 8**
	Create Backup Strategies and Disaster Recovery Plans	8.1 Analyze backup methods and schedules 8.2 Work with the file `Archive` bit for backups and restores 8.3 Perform Volume backups 8.4 Research Storage Area Networks 8.5 Explain off-site backups and data backup integrity testing

Evaluation Process and Grading System:

Evaluation Type	Evaluation Weight
Labs and Assignments	40%
Test #1	30%
Test #2	30%

Date: July 5, 2023

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