MARYMOUNT
UNIVERSITY

School of Business Administration
2018-19 Summer Semester

COURSE SYLLABUS

Course Number IT-530 OL	**Course Title** COMPUTER SECURITY		
Fall Semester	**Spring Semester**	**Summer Semester** XXX	**Credit Hours** 3
Name of Instructor: Dr. Ibrahim Waziri, Jr.			
Meeting Day, Time, and Room Number Online			
Office Hours, Location, Phone: Available by e-mail or appointment as needed			
E-mail/Phone: [redacted]			

UNIVERSITY STATEMENTS

ACADEMIC INTEGRITY

By accepting this syllabus, you pledge to uphold the principles of Academic Integrity expressed by the Marymount University Community. You agree to observe these principles yourself and to defend them against abuse by others. Items submitted for this course may be submitted to TurnItIn.com for analysis.

STUDENT COPYRIGHT INFORMATION

For the benefit of current and future students, work in this course may be used for educational critique, demonstrations, samples, presentations, and verification. Outside of these uses, work shall not be sold, copied, broadcast, or distributed for profit without student consent.

ACCOMMODATIONS AND ACCESSIBILITY CONCERNS

Please address any special challenges or needs with the instructor at the beginning of the semester.

Students with Disabilities

If you are seeking accommodations (class/course adjustments) for a long-term or short-term (less than 6 months) disability, you must do the following:

1) Register as a student with a disability with Student Access Services (SAS) in the Center for Teaching and Learning. This process takes time, so you should engage it as early as possible.
2) Once registered with SAS, you may be approved for accommodations by SAS. Approved accommodations will be listed on a "Faculty Contact Sheet" (FCS). This is important because not all accommodation requests are approved.
3) After receiving the FCS, meet with each of your instructors as soon as possible to review your accommodations, and have them sign the FCS. This document will help you and your instructors develop a plan for providing the approved accommodations.
4) Let SAS know if there are any concerns about the way your accommodations are being implemented by your instructors.

Please remember that:

1) Accommodations for disabling conditions cannot be granted if you do not follow the above steps.
2) Accommodations are not retroactive. That is, accommodations can only be applied to a course *after* they have been approved by SAS and put into motion by *you* through working with your instructors.
3) Appointments with the SAS staff are scheduled through the Starfish "Success Network" tab in Canvas. For more information, check the SAS website, e-mail access@marymount.edu, or call 703-284-1538.

Students with Temporary Challenges

Temporary challenges due to accident, illness, etc. that may result in missing class or navigating general campus access do not fall under the purview of SAS. If you experience something of this nature, please start by alerting your instructors. The Dean of Student Success may be involved in alerting instructors in extreme cases.

EMERGENCY NOTIFICATION POLICY

When students are absent due to a crisis situation or unexpected, serious illness and unable to contact their individual instructors directly, the Division of Student Affairs can send out an Emergency Notification. To initiate an Emergency Notification, students should contact the **Division of Student Affairs** **703-284-1615** or studentaffairs@marymount.edu. Emergency Notifications are **NOT** appropriate for non-emergency situations (e.g. car problems, planned absences, minor illnesses, or a past absence); are **NOT** a request or mandate to excuse an absence, which is at the sole discretion of the instructor; and are **NOT** a requirement for student absences. If a student contacts instructors about an emergency situation directly, it is not necessary to involve the Division of Student Affairs as arrangements are made to resolve the absence.

For non-emergency absences, students should inform their instructors directly.

ACCESS TO STUDENT WORK

Copies of your work in this course including copies of any submitted papers and your portfolios may be kept on file for institutional research, assessment and accreditation purposes. All work used for these purposes will be submitted anonymously.

UNIVERSITY POLICY ON WEATHER AND EMERGENCY CLOSINGS

Weather and Emergency closings are announced on Marymount's web site: **www.marymount.edu**, through **MUAlerts**, area radio stations, and TV stations. You may also call the **Weather and Emergency Hotline at (703) 526-6888** for current status. Unless otherwise advised by local media or by official bulletins listed above, students are expected to report for class as near normal time as possible on days when weather conditions are adverse. Decisions as to inclement closing or delayed opening are not generally made before 6:00 AM and by 3:00 PM for evening classes of the working day. Emergency closing could occur at any time making **MUAlerts** the most timely announcement mechanism. **Students are expected to attend class if the University is not officially closed.** If the University is closed, course content and assignments will still be covered as directed by the course instructor. Please look for communication from course instructor (e.g., Canvas) for information on course work during periods in which the University is closed.

1. BROAD PURPOSE OF COURSE

This course provides an overview for the computer security risks facing enterprises today and covers the many options available for mitigation of these risks. Topics include security concepts, controls, and techniques; standards; designing, monitoring, and securing operating systems; hardware; applications; databases; networks (wired and wireless); and the controls used to enforce various levels of availability, confidentiality and integrity. Computer security is taught in the context of the increasingly global and distributed environment of today's enterprise. Business continuity and disaster recovery planning are also discussed. Prerequisite: IT 520. (3)

2. COURSE OBJECTIVES: Upon successful completion of this course students will be expected to:

a. Explain the goals of computer security and distinguish between common computer security terms;
b. Explain the issues of computer privacy including identity theft;
c. Classify the major threats to computer systems and describe the typical countermeasures;
d. Examine the technological, social, legal, and ethical dimensions of computer security;
e. Make computer security decisions with consideration of their technical, social, legal, and ethical context;
f. Independently research computer security incidents and evaluate them from their technological, social, legal, and ethical perspectives;
g. Evaluate security and privacy policies; and
h. Examine the personnel requirements for an information security office, including researching available certifications.

Specific topic coverage includes:

- Introduction to Information Security
- The Need for Security
- Legal, Ethical, and Professional Issues in Information Security
- Planning for Security
- Risk Management
- Security Technology: Firewalls, VPNs, and Wireless
- Security Technology: Intrusion Detection and Prevention Systems and Other Security Tools
- Cryptography
- Physical Security
- Implementing Information Security
- Security and Personnel
- Information Security Maintenance and eDiscovery

3. TEACHING METHOD

This class will cover a wide array of topics through various methods of instruction; Lectures on material, tool demonstrations, group discussions, and open forums. Classes will be online. Student participation and interaction is required for this course. Assignments throughout the semester are geared towards making the student think critically on the subject matter, learn the aspects of information security, and implement knowledge gained as a security professional.

4. GRADING POLICY

The course will follow the scoring table listed below: All grades will be on Canvas

Category:	*Grade Percentage*
Quizzes	50%
Research Paper/Article Review	20%
Participation/Discussions	20%
Final Exam	10%
Total:	100%

Percentage:	*Letter Grade*
90-100%	A
80-89%	B
70-79%	C
60-69%	D
0-59%	F

Quizzes: There will be ten (10) quizzes provided throughout the semester, one per lecture. The questions will be multiple choice or fill in the blank. The content of each quiz will be focused on its corresponding lecture. You must complete a quiz before the next module unlocks. Quizzes constitute 50% of your grade. Students must complete every quiz in one sitting. Student will NOT be able to retake an attempted quiz.

Research Paper/Article Review: Students are expected write a half page word document (New Times Roman, 12 font size, 1.15 line space, using default MS Word margin) review for any research paper or article related to the subsequent lecture. Students can use Marymount library resources, Google Scholar, etc. (No Wikipedia) to find papers/articles. Each review paper must have an APA referencing of the research paper or article being reviewed. Review Papers constitute 20% of your grade.

Participation/Discussions: For every lecture/module, there will be a discussion board. Students are expected to participate in the discussion board by asking one question and answering a question or providing more insight to the question asked. Questions and answers available in the text/lecture do NOT qualify as discussion. An example "What is Cybersecurity" or "What is the difference between Confidentiality and Integrity" do NOT qualify. Discussions constitute 20% of your grade.

Final Exam: The final exam will be multiple choice or fill in the blank and based on the textbook, lectures, and quizzes. The Exams will be available on **July 29th, 2019 at 12:00AM and will close on August 3rd, 2019 at 11:59PM.** Students MUST take and complete in one sitting before the exams closes. Final Exams constitute 10% of your grade.

5. CLASS SCHEDULE

Lecture modules unlocks every Monday, but only after a student completes the previous module all previous module task.

Module	Topics	Task
Module 1 **Week 1**	Introduction – Review of Syllabus	• Introduce yourself • Buy the textbook • Familiarize yourself with the syllabus, class content, deliverables and expectations. • Ask questions. • Read next week chapters.
Module 2 **Week 2**	Chapter 1: Introduction to Information Security History & Definition of Information Security NSTISSC Security Model, ISO 27001 ISMS, CoBIT, NIST 800-53, NIST CSF Critical Characteristics of Information Information Security Models Balancing Security and Access Security SDLC Communities of Interest	• Take Quiz • Participate in Discussions • Submit Review Paper • Read Next Week Chapter
Module 3 **Week 3**	Chapter 2: The Need for Security Review of Security Incidents Business vs Technology Threats to and Vulnerabilities of Systems Known Attacks Malicious Code Denial-of-Service Spoofing Social Engineering	• Take Quiz • Participate in Discussions • Submit Review Paper • Read Next Week Chapter(s)
Module 4 **Week 4**	Chapter 3: Legal, Ethical, and Professional Issues in Information Security Laws and Regulations Related to InfoSec Ethical Issues in InfoSec	• Take Quiz • Participate in Discussions • Submit Review Paper

	Operations Legal Elements (investigative authorities) Types of Law Relevant U.S. laws Policy vs Law & International Laws Codes of Ethics Need for Legal Counsel Chapter 5: Risk Management Risk Identification Threat/Vulnerability Assessment Cost/Benefit Analysis Risk Mitigation (implementing and maintaining)	• Read Next Week Chapter(s)
Module 5 **Week 5**	Chapter 6: Security Technology: Firewalls and VPNs Authentication Access Control Firewall types and operations Remote access Virtual private networks Other Topics: CVSS Model 3, STRIDE / DREAD	• Take Quiz • Participate in Discussions • Submit Review Paper • Read Next Week Chapter
Module 6 **Week 5**	Chapter 7: Security Technology: IDS & Prevention Systems Intrusion Detection and Access Control Techniques Intrusion Detection Systems Intrusion Prevention Systems Honeypots and Honeynets Access Control Techniques Biometrics	• Take Quiz • Participate in Discussions • Submit Review Paper • Read Next Week Chapter
Module 7 **Week 6**	Chapter 8: Cryptography Encryption and Decryption Poly-alphabetic ciphers History of Cryptology Symmetric Ciphers Public Key Systems (RSA) Hash functions (SHA, MD5) Cryptographic Applications Protocols (SSL/TSL) Digital signatures and certificates	• Take Quiz • Participate in Discussions • Submit Review Paper • Read Next Week Chapter
Module 8 **Week 7**	Chapter 4: Planning for Security Security planning Security Policy Project management Incident response Business Continuity Planning Disaster Recovery Incident Response Contingency Planning	• Take Quiz • Participate in Discussions • Submit Review Paper • Read Next Week Chapter(s)
Module 9 **Week 8**	Chapter 9: Physical Security Physical access control (locks, cards) Fire safety methods Building construction Power controls (ups, etc.) Environmental controls (HVAC, etc.) Chapter 10: Implementing Information Security Information Security Project Management Technical Aspects of Implementation Non-Technical Aspects of Implementation Information Systems Security Certification & Accreditation	• Take Quiz • Participate in Discussions • Submit Review Paper • Read Next Week Chapter(s)
Module 10 **Week 9**	Chapter 11: Security & Personnel Personnel Security Practices and Procedures Authentication and Authorization Security Training Security Awareness Training	• Take Quiz • Participate in Discussions • Submit Review Paper • Read Next Week Chapter

	Need-to-know, Rotation and Minimal Access Principles Background Checks Security Clearances	
Module 11 **Week 10**	Chapter 12: Information Security Maintenance Maintaining a Secure Environment Maintenance Model Configuration Management Change management Updates, patches and fixes Monitoring and auditing System Life Cycle	• Take Quiz • Participate in Discussions • Submit Review Paper • Open the Review Module
Module 12 **Week 10**	Review and Extra Credit assessment	• Participate in Review • Ask questions (if any) • Take or Submit Extra Credit assessment.
Module 13 **Week 11**	**Final Exam**	• **TAKE EXAMS BEFORE Aug 3rd 11:59 PM**

6. REQUIRED TEXT

Principles of Information Security, Sixth Edition
Michael E. Whitman and Herbert J. Mattord
ISBN-13: 978-1-337-10206-3

Students can also use the previous 5th Edition.

Principles of Information Security, Fifth Edition
Michael E. Whitman and Herbert J. Mattord
ISBN-13: 978-1-285-44836-7
ISBN-10: 1-285-44836-7