Chair: Tracy Christofero | **GC#6: Course Addition**

Request for Graduate Course Addition

1. Prepare one paper copy with all signatures and supporting material and forward to the Graduate Council Chair.
2. E-mail one identical PDF copy to the Graduate Council Chair. If attachments included, please merge into a single file.
3. ***The Graduate Council cannot process this application until it has received both the PDF copy and the signed hard copy.***

College: CITE Dept/Division: Computer Science Alpha Designator/Number: CYBR/510 (•) Graded ( ) CR/NC

Contact Person: Dr. Wook-Sung Yoo Phone: x5452

NEW COURSE DATA:

New Course Title: Introduction to Cyber Security

Alpha Designator/Number: C Y B R / 5 1 0

Title Abbreviation: I n t r o t o C y b e r S e c u r i t y

(Limit of 25 characters and spaces)

Course Catalog Description: (Limit of 30 words)
This course provides an overview of the cybersecurity field, the basic foundations of the current technology and its impacts along with the predominant threat components and remediation.

Co-requisite(s): None First Term to be Offered: Spring 2019

Prerequisite(s): None Credit Hours: 3

Course(s) being deleted in place of this addition (*must submit course deletion form*): NA

Signatures: if disapproved at any level, do not sign. Return to previous signer with recommendation attached.

Dept. Chair/Division Head Yoo, Wook	Date 9/17/18
Registrar 110101	Date 9/21/18
College Curriculum Chair	Date 9/28/18
Graduate Council Chair	Date

Request for Graduate Course Addition - Page 2

College: CITE | Department/Division: Computer Science | Alpha Designator/Number: CYBR/510

Provide complete information regarding the new course addition for each topic listed below. Before routing this form, a complete syllabus also must be attached addressing the items listed on the first page of this form.

1. FACULTY: Identify by name the faculty in your department/division who may teach this course.

Paulus Wahjudi, Ph.D.
Cong Pu, Ph.D.

2. DUPLICATION: If a question of possible duplication occurs, attach a copy of the correspondence sent to the appropriate department(s) describing the proposal. Enter "***Not Applicable***" if not applicable.

Not Applicable

3. REQUIRED COURSE: If this course will be required by another deparment(s), identify it/them by name. Enter "***Not Applicable***" if not applicable.

Not Applicable

4. AGREEMENTS: If there are any agreements required to provide clinical experiences, attach the details and the signed agreement. Enter "***Not Applicable***" if not applicable.

Not Applicable

5. ADDITIONAL RESOURCE REQUIREMENTS: If your department requires additional faculty, equipment, or specialized materials to teach this course, attach an estimate of the time and money required to secure these items. (Note: Approval of this form does not imply approval for additional resources.) Enter "***Not Applicable***" if not applicable.

Not Applicable

6. COURSE OBJECTIVES: (May be submitted as a separate document)

Please see attached document

7. COURSE OUTLINE (May be submitted as a separate document)

Please see attached document

8. SAMPLE TEXT(S) WITH AUTHOR(S) AND PUBLICATION DATES (May be submitted as a separate document)

Please see attached document

9. EXAMPLE OF INSTRUCTIONAL METHODS (Lecture, lab, internship)

Please see attached document

10. EXAMPLE EVALUATION METHODS (CHAPTER, MIDTERM, FINAL, PROJECTS, ETC.)

Exam, Homework Assignments and Projects

11. ADDITIONAL GRADUATE REQUIREMENTS IF LISTED AS AN UNDERGRADUATE/GRADUATE COURSE

Not applicable

12. PROVIDE COMPLETE BIBLIOGRAPHY (May be submitted as a separate document)

Please see attached document

Request for Graduate Course Addition - Page 5

Please insert in the text box below your course summary information for the Graduate Council agenda. Please enter the information exactly in this way (including headings):

Department:
Course Number and Title:
Catalog Description:
Prerequisites:
First Term Offered:
Credit Hours:

Department: Computer Science
Course Number and Title: CYBR 510 Introduction to Cyber Security
Catalog Description: This course provides an overview of the cybersecurity field, the basic foundations of the current technology and its impacts along with the predominant threat components and remediation.
Prerequisites: None
First Term Offered: Spring 2019
Credit Hours: 3

BIBLIOGRAPHY

Principles of Computer Security, Fourth Edition (Official Comptia Guide) 4th Edition by Wm. Arthur Conklin ISBN-13: 978-0071835978 ISBN-10: 0071835970

Computer Security: Principles and Practice (4th Edition) 4th Edition by William Stallings ISBN-13: 978-0134794105 ISBN-10: 0134794109

CYBR 510 Introduction to Cyber Security

Course Title/Number	Introduction to Cyber Security /CYBR 510
Semester/Year	Spring/2019
Days/Time	TBD
Location	TBD
Instructor	Dr. Cong Pu
Office	WAEC 3109
Phone	(304)696-6204
E-Mail	puc@marshall.edu
Office Hours	TBD
University Policies	By enrolling in this course, you agree to the University Policies listed below. Please read the full text of each policy by going to www.marshall.edu/academic-affairs and clicking on "Marshall University Policies." Or, you can access the policies directly by going to www.marshall.edu/academic-affairs/policies/. Academic Dishonesty/Excused Absence Policy for Undergraduates/Computing Services Acceptable Use/Inclement Weather/Dead Week/Students with Disabilities/Academic Forgiveness/Academic Probation and Suspension/Academic Rights and Responsibilities of Students/Affirmative Action/Sexual Harassment

Course Description

This course provides an overview of the cybersecurity field, the basic foundations of the current technology and its impacts along with the predominant threat components and remediation.

Course Student Learning Outcomes

Course Student Learning Outcomes	How students will practice each outcome in this Course	How student achievement of each outcome will be assessed in this Course
Students will be able to discuss the various aspects in physical and cyber security, its weaknesses and ways to mitigate	Homework assignments, In class examples, Group discussions	Graded exam problems Graded homework assignments
Students will be able to discuss and utilize techniques to find vulnerabilities in an environment and develop reasonable solutions	Homework Assignments, In class examples Group discussions	Graded exam problems Graded homework assignments
Students will be able to explain the basics and perform fundamental analysis on the likelihood of an attack against an environment	Homework, In class examples	Graded exam problems Graded homework assignments

Required Texts, Additional Reading, and Other Materials

Required Text

Principles of Computer Security, Fourth Edition (Official Comptia Guide) 4th Edition by Wm. Arthur Conklin ISBN-13: 978-0071835978 ISBN-10: 0071835970

Additional Text

Computer Security: Principles and Practice (4th Edition) 4th Edition by William Stallings ISBN-13: 978-0134794105 ISBN-10: 0134794109

Course Requirements / Due Dates

Interim Examinations

There will be two exams, midterm and final exams.

Homework Assignments

Homework problems will be assigned regularly and must be completed individually.

Class Projects

Class Projects are done in teams and focus on specific objectives.

Late Submission Policy

No Late submission will be accepted

Attendance Policy

Missing more than 3 classes will result in a 10 points reduction from your final grade.

Grading Policy

Activity	Points
Attendance and Participation	10
Midterm Exam	25
Homework Assignments	20
Class Projects	20
Final Exam	25
Total	100

Course grades are awarded based on the following scheme:

Score	Letter Grade
>= 90	A
>= 80 & < 90	B
>= 70 & < 80	C
>= 60 & < 70	D
< 60	F

Course Schedule

This is the list of topics. This could be adjusted as the semester progresses at the discretion of the instructor. Lecture slides will be posted to MUOnline.

Week	Schedule
1	General Security Concepts
2	Privacy, Legal Issues and Ethics
3	Operational and Organizational Security
4	Cryptography
5	Public Key Infrastructure
6	Physical Security
7	Midterm Exam
8	Network Fundamentals
9	Infrastructure Security
10	Wireless Security
11	Intrusion Detection Systems
12	System Hardening and Baselines
13	Types of Attacks
14	Secure Software Development
15	Disaster Recovery and Risk Management