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/535   ● Graded ○ CR/NC

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

NEW COURSE DATA:

New Course Title: Cyber Risk

Alpha Designator/Number: | C | Y | B | R | / | 5 | 3 | 5 | |

Title Abbreviation: | C | y | b | e | r | | R | i | s | k | | | | | | | | | | | | | | | |

(Limit of 25 characters and spaces)

Course Catalog Description: (Limit of 30 words)

The functions and purposes of the latest developments in cybersecurity are covered. Topics includes design, implementation, and testing industrial networks and applications to ensure their security and reliability.

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

Prerequisite(s): CYBR 510   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 _____   Date 9/17/18

Registrar _____   110101   Date 9/21/18

College Curriculum Chair _____   Date 9/26/18

Graduate Council Chair _____   Date _____

College: CITE   Department/Division: Computer Science   Alpha Designator/Number: CYBR/535

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
Husnu Narman, 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 535 Cyber Risk
Catalog Description: The functions and purposes of the latest developments in cybersecurity are covered. Topics include design, implementation, and testing industrial networks and applications to ensure their security and reliability.
Prerequisites: CYBR 510
First Term Offered: Fall 2019
Credit Hours: 3

BIBLIOGRAPHY

- Alshanetsky, Ilia. PHP/architect's guide to PHP security. Toronto: Marco Tabini & Associates, 2005. Print.
- Connor, T. J. Violent Python a cookbook for hackers, forensic analysts, penetration testers and security engineers. Waltham, MA: Syngress, 2013. Print.
- Kennedy, David. Metasploit : the penetration tester's guide. San Francisco: No Starch Press, 2011. Print.
- McClure, Stuart, et al. Hacking exposed 7: network security secrets & solutions. New York: McGraw-Hill, 2012. Print.
- Sanders, Chris. Practical packet analysis using Wireshark to solve real-world network problems. San Francisco, CA: No Starch Press, 2011. Print.
- Seitz, Justin. Gray hat Python Python programming for hackers and reverse engineers. San Francisco: No Starch Press, 2009. Print.

CYBR 535 Cyber Risk

Course Title/Number	Cyber Risk /CYBR 535
Semester/Year	Fall/2019
Days/Time	TBD
Location	TBD
Instructor	Dr. Paulus Wahjudi
Office	WAEC 3113
Phone	(304)696-5443
E-Mail	wahjudi@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

The functions and purposes of the latest developments in cybersecurity are covered. Topics includes design, implementation, and testing industrial networks and applications to ensure their security and reliability. (PR: CYBR 510).

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
Design, develop and implement a secure Cyber-infrastructure and Security Operation Center.	Homework assignments, In class examples, Group discussions	Exam problems Homework assignments Class Project
Assess network defenses and computer system's security vulnerabilities and detect attempted security breaches using appropriate tools and resources.	Homework Assignments, In class examples Group discussions	Exam problems Homework assignments Class Project
Utilize security technologies such as firewalls, VPNs, virtualization, virus	Homework, In class examples	Exam problems Homework assignments

scanning, intrusion protection and patches to industrially harden a cyber-infrastructure.	Class Project

Required Texts, Additional Reading, and Other Materials

Required Text

Stuttard, Dafydd, and Marcus Pinto. The web application hacker's handbook finding and exploiting security flaws. Indianapolis: Wiley, 2011. Print.

Additional Text

- Sanders, Chris. Practical packet analysis using Wireshark to solve real-world network problems. San Francisco, CA: No Starch Press, 2011. Print.
- Seitz, Justin. Gray hat Python Python programming for hackers and reverse engineers. San Francisco: No Starch Press, 2009. Print.

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	Understanding Cyber Risk
2	Virtualization & Hypervisor
3	Network Scanning and Forensics
4	Honeypot and Tarpit
5	Public Key Infrastructure
6	Trojan Horse and Rootkit
7	Midterm Exam
8	Intrusion Detection and Penetration Testing
9	Software as a Service and System Hardening
10	Cyber Defense and Offense
11	Switch management and ARP attacks
12	Wireless Security
13	Software as a Service
14	Secure Software Development
15	Information Security and Assurance