Agenda Item #16-13
Effective: Fall 2017

Eastern Illinois University

New/Revised Course Proposal Format

(Approved by CAA on 4/3/14 and CGS on 4/15/14, Effective Fall 2014)

Banner/Catalog Information (Coversheet)

1. **_X__New Course or _____Revision of Existing Course**
2. **Course prefix and number:** __CYB 5900_____
3. **Short title:** __Cybersecurity Capstone_____
4. **Long title:** __Cybersecurity Capstone _____
5. **Hours per week:** _0_ Class _5.0_ Lab _2_ Credit
6. **Terms:** ___ Fall ___ Spring ___ Summer _X_ On demand
7. **Initial term**: _X_ Fall ___ Spring ___ Summer Year: _2017_
8. **Catalog course description:**

   In this course, students integrate concepts from previous coursework and experience into a comprehensive security strategy for information systems. The security topics include system architecture, security models, vulnerability assessment, threat analysis, incident detection, and response.

9. **Course attributes:**

   General education component: __None_____

   ___ Cultural diversity ___ Honors ___ Writing centered ___ writing intensive ___Writing active

10. **Instructional delivery**
    Type of Course:

    ___ Lecture _X__ Lab __ Lecture/lab combined ___ Independent study/research

    ___ Internship ___ Performance ___ Practicum/clinical ___ other, specify: _____

    Mode(s) of Delivery:

    __ Face to Face ___ Online ___ Study Abroad

    _X_ Hybrid, specify approximate amount of on-line and face-to-face instruction: about 50% face-to-face and 50% online instructions

11. **Course(s) to be deleted from the catalog once this course is approved.** __None_____
12. **Equivalent course(s):** __None_____

    a. Are students allowed to take equivalent course(s) for credit? ___ Yes X_ No

13. **Prerequisite(s):** __MIS 4860, CYB 5550_____

    a. **Can prerequisite be taken concurrently?** ___ Yes _X_ No

    b. **Minimum grade required for the prerequisite course(s)?** _C_

    c. **Use Banner coding to enforce prerequisite course(s)?** _X_ Yes ___ No

    d. **Who may waive prerequisite(s)?**

    ___ No one _X_ Chair ___ Instructor ___ Advisor ___ Other (specify)

14. **Co-requisite(s):** __None_____

15. **Enrollment restrictions**

    a. **Degrees, colleges, majors, levels, classes which <u>may</u> take the course:** __Graduate students in the M.S. in Cybersecurity or related programs as determined by the School of Technology Graduate Coordinator__

    b. **Degrees, colleges, majors, levels, classes which may <u>not</u> take the course:** _____

16. **Repeat status:** _X_ May not be repeated ___ May be repeated once with credit

17. **Enter the limit, if any, on hours which may be applied to a major or minor:** _2_

18. **Grading methods:** _X_ Standard ___ CR/NC __ Audit ___ ABC/NC

19. **Special grading provisions:**

    ___ Grade for course will <u>not</u> count in a student's grade point average.

    ___ Grade for course will <u>not</u> count in hours toward graduation.

    ___ Grade for course will be removed from GPA if student already has credit for or is registered in: _____

    ___ Credit hours for course will be removed from student's hours toward graduation if student already has credit for or is registered in: _____

20. **Additional costs to students:**
    Supplemental Materials or Software_____

    Course Fee _X_ No ___Yes, Explain if yes_____

21. **Community college transfer:**

    ___ A community college course may be judged equivalent.

    _X_ A community college may <u>not</u> be judged equivalent.

    Note: Upper division credit (3000+) will <u>not</u> be granted for a community college course, even if the content is judged to be equivalent.

Rationale, Justifications, and Assurances (Part I)

1. _X_ Course is required for the major(s) of __Master of Science in Cybersecurity_____
   ___Course is required for the minor(s) of _____
   ___Course is required for the certificate program(s) of _____
   ___ Course is used as an elective
2. **Rationale for proposal** :

   The School of Technology, in cooperation with School of Business, is developing a new Master of Science program in Cybersecurity to respond to this workforce demand. This course will provide intensive security content and hands-on experience to students. Students will gain practical experience on securing a computer information system while maintaining necessary services. Students will have residency on campus because they need to manage, program and experiment with the advanced cybersecurity equipment in our laboratories. According to the Bureau of Labor Statistics' Occupational Outlook Handbook, employment of information security analysts is expected to rise "much faster than average" (37%) from 2012-2022, with median salary currently at $86,170 per year. Additionally, employment of information security analysts in Illinois is among the top quartile of all states in the U.S.

3. **Justifications for (answer N/A if not applicable)**

   Similarity to other courses:

   N/A

   Prerequisites: Students are expected to integrate concepts from previous coursework and experience; therefore, courses listed in item 13 of "Banner/Catalog Information (Coversheet)" are required.

   Co-requisites: N/A

   Enrollment restrictions: This is a graduate level course and is restricted to graduate students. The restrictions help ensure those taking the class are adequately prepared.

   Writing active, intensive, centered: No
4. **General education assurances (answer N/A if not applicable)**

   General education component: N/A

Curriculum: N/A

Instruction: N/A

Assessment: N/A

5. **Online/Hybrid delivery justification & assurances (answer N/A if not applicable)**

Online or hybrid delivery justification:

One of EIU's missions is to provide accessible education. EIU constantly enrolls a considerable number of nontraditional students, such as working professionals, distant residents, and international learners. This course can be technology delivered to that population, who otherwise couldn't access the course or would look for alternative institutions.

Instruction:

The course will be delivered in an on-line Learning Management System (LMS). Learning materials, discussions, assignments, and grading will all be placed on the LMS. The contents of this course are naturally suitable for technology delivery. Teaching materials are in forms of presentation slides, word document, etc. Student work is in digital formats such as script code, database files, and word documents.

Any instructors of technology-delivered courses/sections must submit proof of having completed the Online Course Development Institute (OCDI), Illinois Online Network's "Master Online Teacher" certificate or another documented and equivalent training activity before teaching the courses/sections for the first time.

Integrity:

The instructor will verbally interview students and ask questions about assignments to assure their integrity. Tests may use a face-to-face format or use web conferencing software (virtual classroom with audio/video and white board support).

Interaction:

In addition to email, online discussions, and social networks, class interaction will go through web conferencing software in real time.

Model Syllabus (Part II)

Please include the following information:

1. Course number and title
2. Catalog description
3. Learning objectives.
4. Course materials.
5. Weekly outline of content.
6. Assignments and evaluation, including weights for final course grade.
7. Grading scale.
8. Correlation of learning objectives to assignments and evaluation.

1. Course Number and Title

CYB 5900 – Cybersecurity Capstone

2. Catalog Description

In this course, students integrate concepts from previous coursework and experience into a comprehensive security strategy for information systems. The security topics include system architecture, security models, vulnerability assessment, threat analysis, incident detection and response.

3. Learning Objectives

Upon completion of this course, students will be able to:

#	**Objectives**	Graduate Learning Goals
1	Explain functions, strengths, and weaknesses of common cryptography methods.	a. Depth of content knowledge b. Effective critical thinking and problem solving c. Effective oral and written communication
2	Explain authentication, access control, and intrusion detection mechanisms.	a. Depth of content knowledge b. Effective critical thinking and problem solving c. Effective Oral and Written communication
3	Describe how malware and hackers carry out network attacks.	a. Depth of content knowledge b. Effective critical thinking and problem solving c. Effective Oral and Written communication
4	Identify software security solutions and network defenses.	a. Depth of content knowledge b. Effective critical thinking and problem solving
5	Analyze physical and infrastructure security technologies.	a. Depth of content knowledge b. Effective critical thinking and problem solving

6	Perform IT risk assessments and security audits.	a. Depth of content knowledge b. Effective critical thinking and problem solving c. Effective oral and written communication
7	Identify and explain legal mandates and ethical information security practices.	a. Depth of content knowledge b. Effective critical thinking and problem solving
8	Develop organizational security policies and plans.	a. Depth of content knowledge b. Effective critical thinking and problem solving c. Effective oral and written communication d. Evidence of advanced scholarship through research and/or creative activity

4. Course Materials

- Two textbooks from previous courses
  - "Principles of Computer Security CompTIA Security+ and Beyond (Exam SY0-301), 3rd Edition (Official CompTIA Guide)" by Arthur Conklin and Gregory White. McGraw Hill 2012
  - "CISSP All-In-One Exam Guide [With CDROM] Hardcover", October 18, 2012 by Shon Harris, John Wiley and Sons.
- Online resources such as http://certification.comptia.org and www.isc2.org.

5. Weekly Outline of Content:

Modules	Topics	Time
1	Setting up cloud server and managing security on cloud servers such as Microsoft cloud 12.8.	8 hours
2	Setting up firewall architectures on firewalls like Palo-alto and CISCO. Analyzing the logs of firewalls.	8 hours
3	Setting up networks/servers protected by a specific architecture.	8 hours
4	Utilizing advanced sniffers and protocol readers to analyze sessions/passwords.	8 hours
5	Detecting signs of intrusion that may jeopardize the confidentiality, integrity, availability and control of networks. Analyzing packet activity for indications of network attack.	8 hours
Final Project/Cybersecurity War Game	Stage 1: Setting up server that hosts common services such as Web, email, FTP, and database. Stage 2: Using hacking/administration tools to probe other groups' servers and discover their vulnerabilities. Stage 3: Fixing discovered vulnerabilities.	32 hours
Report/Presentation	Writing report and presenting to class.	8 hours

6. Assignments and Evaluation, Including Weights for Final Course Grade

Grades will be based upon the following proportions:

- Quizzes 10%
- Module Activities 40%
- Final Project 30%
- Report/Presentation 20%

7. Grading Scale

Final grades are based on the following scale:

- Percentage ≥ 90 A
- $80 \leq$ Percentage < 90 B
- $70 \leq$ Percentage < 80 C
- $60 \leq$ Percentage < 70 D
- Percentage < 60 F

8. Correlation of Learning Objectives to Assignments and Evaluation

Objective	Quizzes	Module Activities	Final Projects / War Game	Report / Presentation
1	X			X
2	X			X
3	X	X	X	X
4	X	X	X	X
5	X	X	X	X
6	X	X	X	X
7	X	X	X	X
8	X	X	X	X

Date approved by the department or school: NOVEMBER 22, 2015
Date approved by the college curriculum committee: JANUARY 22, 2016
Date approved by CGS: