Eastern Illinois University
Revised Course Proposal
MIS 4850, Systems Security

Agenda Item #15-134
Effective Spring 2016
Effective Fall 2016, with revisions

Banner/Catalog Information (Coversheet)

1. **____New Course or __X__Revision of Existing Course**

2. **Course prefix and number:** _MIS 4850_____

3. **Short title:** _Systems Security_____

4. **Long title:** _Systems Security_____

5. **Hours per week:** _3_ Class _0_ Lab _3_ Credit

6. **Terms:** ___ Fall ___ Spring ___ Summer _X__ On demand

7. **Initial term**: ___ Fall _X_ Spring ___ Summer Year: _2016_

8. **Catalog course description:** Study of theories, principles and techniques of information systems security. The course covers basic security concepts, communications security, infrastructure security, cryptography, as well as operational and organizational security.

9. **Course attributes:**

   General education component: _____N/A_____

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

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

    _X_ Lecture ___ Lab ___ Lecture/lab combined ___ Independent study/research

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

    Mode(s) of Delivery:

    _X_ Face to Face _X_ Online ___ Study Abroad

    _X_ Hybrid, specify approximate amount of on-line and face-to-face instruction: A maximum of 49% of the course will be online.

11. **Course(s) to be deleted from the catalog once this course is approved.** None. This is a revision of an existing course.

12. **Equivalent course(s):** _____None_____

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

13. **Prerequisite(s):** Junior, Senior or Graduate standing, BUS 3500 or ACC 3900, or permission of the Associate Chair, School of Business.

    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 ___ Chair ___ Instructor ___ Advisor _X_ Other (specify): Associate Chair

14. Co-requisite(s): _____None_____

15. Enrollment restrictions

a. Degrees, colleges, majors, levels, classes which <u>may</u> take the course: __Junior, Senior, or Graduate Student_____

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

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: _3_

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_____NONE_____

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 (pending approval)_

   ___Course is required for the minor(s) of _____

   ___Course is required for the certificate program(s) of _____

   _X_ Course is used as an elective __for MIS Major, MIS Minor, and MBA_____

2. **Rationale for proposal**: This is an update of an existing course in the MIS curriculum which allows sections to be taught through hybrid or online formats in keeping with the university's online delivery initiatives. Information Systems Security is one of the key issues facing organizations' IT infrastructure today. In order to be successful in today's job market, MIS graduates seeking a career in the Systems Security field must understand and know how to plan and manage information security challenges. This class is designed to help students achieve that goal.

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

   Similarity to other courses: N/A

   Prerequisites: Students enrolled in this class must have a good understanding of information systems and network operation. As a result, a successful completion of BUS 3500 or ACC 3900 is necessary.

   Co-requisites: NONE

   Enrollment restrictions: This course builds on material from BUS 3500 or ACC 3900; both of those courses (or their prereqs) require junior status.

   Writing active, intensive, centered: N/A

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: This course will be required in the Online Master of Science in Cybersecurity. Offering and instructing this course through a hybrid or online model also allows and increases the enrollment probability of students in the Summer semester who have moved away from campus and may attempt an equivalent course at another institution. An online course gives EIU the opportunity to market to these students as well as other students interested in taking the course in an alternative format. EIU School of Business continues to deliver high quality education through traditional methods of teaching and technologically advanced methods such as online and hybrid education.

   Instruction: Lectures from the face-to-face courses may be recorded and posted online for students to view. Other online components (e.g., tutorials, videos, discussions) will be included. All faculty who will deliver this course online are/will be OCDI (or appropriate equivalent) trained. Students are able to watch recorded videos whenever they prefer, stop

the video, take notes and ask questions of the instructor and their peers. Systems Security content is suitable for online or hybrid education.

Integrity: Students will take exams through an online test-taking monitoring system, or they will take them at a proctored facility such as a community college in their area.

Interaction: At the discretion of the faculty, provisions and requirements would vary but generally will utilize Email, Web-Based Discussions, and Web-conferencing.

Model Syllabus (Part II)

Please include the following information:

1. Course number and title
MIS 4850 Systems Security

2. Catalog description
Study of theories, principles and techniques of information systems security. The course covers basic security concepts, communications security, infrastructure security, cryptography, as well as operational and organizational security.

3. Learning objectives.
Upon successful completion of the course, students will be able to:

1) Implement basic principles of network security. (CT 5-6), (Graduate 1,2)
2) Evaluate the various types of intrusions and attacks against computers and network systems. (WR 1-3, CT 3), (Graduate 1,2)
3) Analyze and choose the tools and technologies used for providing security. (CT 1-4), (Graduate 1,2)
4) Evaluate security policies, disaster recovery, and computer forensics. (CT 1-4), (Graduate 1,2)
5) Explain cryptography and its applications to the security of networks and operating systems. (CT 1-4), (Graduate 1,2)

4. Course materials.
- *Corporate Computer Security* by Randall Boyle and Raymond R. Panko, 4th edition, Pearson, 2014, ISBN-13: 9780133545197
- Current academic literature on information systems' security such as:
  - Spears, J. and Barki, H. (2010). User Participation in Information Systems Security Risk Management, *MIS Quarterly*, Vol. 34 Issue 3, 503-522.
  - Chickowski, E. (2013, May). The Future of Web Authentication, *Security Dark Reading*, 1-11.

5. Weekly outline of content.

Week	**Topic**	**75-minute class period equivalents**
1	Introduction to computer and network security	2 periods
2	Security goals and the Plan-Protect-Respond cycle	2 periods
3-4	Managing the *security* function (control principles, risk analysis, vulnerability testing)	4 periods
5-6	Incident and disaster response management	4 periods
7-8	Access control and site security	4 periods
9	Attack methods	2 periods
10	TCP/IP Internetworking	2 periods
11-12	Tools and technologies for providing computer and network security	4 periods
13-14	Cryptography and cryptographic systems	4 periods
15	Application security: electronic commerce and email	2 periods
16	Final Exam	2 hours
	Total	**Thirty 75-minute periods + Two hours of final exam**

6. Assignments and evaluation, including weights for final course grade.
Grade weighting may vary by instructor, but it is generally considered as follows:
Undergraduates:

- Exams (40% of total grade)
- Assignments (30% of total grade)
- Case Study on current Information Security issues (15% of total grade)
  Sample Case Study: Student will be asked to analyze a given Information Security infrastructure in light of what they have learned in class in order to discover and lay out the strengths and weaknesses of the infrastructure.
- Final Exam (15% of total grade)

Graduates

- Exams (40% of total grade)
- Assignments (20% of total grade)
- Research Project (25% of total grade)
  Sample Research Project: Student will be asked to analyze a given Information Security infrastructure in light of what they have learned in class in order to discover and lay out the strengths and weaknesses of the infrastructure. Students will then search academic and professional journals (such as Management Information Systems Quarterly, Journal of Computer Security, IEEE Transactions on Information Forensics and Security, and similar) in order to write a research paper providing a theoretical background about the weaknesses found and proposing possible solutions that can be adopted to mitigate risks of attacks.
- Final Exam (15% of total grade)

7. Grading scale.

90% or better	A
80-89%	B
70-79%	C
60-69%	D
Less than 60%	F

8. Correlation of learning objectives to assignments and evaluation.
The students' achievement of the stated course objectives will be assessed as follow:

Objectives	**Exams**	**Assignments**	**Research Project (Grad) or Case Study (UG)**	**Final Exam**
1	X	X		X
2	X	X	X	X
3	X	X	X	X
4	X	X	X	X
5	X			X

Date approved by the discipline: Approved by MIS/OM Discipline on March 24, 2015
Date approved by the department or school: Sch of Business Graduate Committee, April 7, 2015
Date approved by the department or school: Sch of Business Curriculum Committee, April 29, 2015
Date approved by the college curriculum committee: September 23, 2015
Date approved by the Honors Council ***(if this is an honors course):***
Date approved by CAA: October 8, 2015 **CGS:** October 20, 2015