1. **COURSE ID:** CIS 480   **TITLE:** Enterprise Security Policy Management
   Units: 3.0 units   **Hours/Semester:** 48.0-54.0 Lecture hours; and 96.0-108.0 Homework hours
   Method of Grading: Grade Option (Letter Grade or Pass/No Pass)
   Prerequisite: CIS 151, **Corequisite:** CIS 479
   Recommended Preparation:
   >Eligibility for ENGL 838 or ENGL 848 or ESL 400.
   >CIS 110

2. **COURSE DESIGNATION:**
   Degree Credit
   Transfer credit: CSU

3. **COURSE DESCRIPTIONS:**
   Catalog Description:
   >Concepts of how to secure an enterprise by creating a security policy and developing procedures to maintain that security policy. Perform risk analysis and assessment on enterprise security. System Administrators, IT Managers, and Analysts would benefit from this course, as well as Technologists wanting to broaden their impact.

4. **STUDENT LEARNING OUTCOME(S) (SLO'S):**
   Upon successful completion of this course, a student will meet the following outcomes:
   1. Create and refine enterprise security policy and procedures.
   2. Create tools to track risks, document and mitigate them.

5. **SPECIFIC INSTRUCTIONAL OBJECTIVES:**
   Upon successful completion of this course, a student will be able to:
   1. Develop and refine a security policy in context of an enterprise.
   2. Propose recommendations on how to address security problems at a company and update security policy to implement recommendations.
   3. Perform risk analysis and assessment based on the security policy and document exceptions and document a risk assessment and mitigation strategy.
   4. Survey implementation of the security policy using the compiled risk assessment strategy to document and report on areas in implementation that do not follow security policy procedures.
   5. Document high-level recommendations to align the requirements of the security policy with its implementation, and with critical business requirements.

6. **COURSE CONTENT:**
   Lecture Content:
   >A. Develop and refine security policy and procedures
   1. Develop and refine a security policy in context of an enterprise as a whole looking for omissions, contradictions, tenability, and errors.
   2. Propose recommendations on how to address security problems at a company and update security policy to implement recommendations.
   3. Produce a work plan to validate and implement documented recommendations.
   >B. Perform risk analysis and assessment based on the security policy and document exceptions
   1. Document a risk assessment and mitigation strategy.
   2. Survey implementation of the security policy using the compiled risk assessment strategy to document and report on areas in implementation that do not follow security policy procedures.
   3. Document high-level recommendations to align the requirements of the security policy with its implementation, and with critical business requirements being mindful of information from technical personnel like Network Engineers, Programmers and Database Professionals.

7. **REPRESENTATIVE METHODS OF INSTRUCTION:**
   Typical methods of instruction may include:
   A. Lecture
   B. Critique

    C. Activity
    D. Discussion
    E. Guest Speakers
    F. Observation and Demonstration
    G. Other (Specify): In class problem-solving. Class (group) problem-solving. Q/A sessions with students. Quiz and examination review performed in class.

8. **REPRESENTATIVE ASSIGNMENTS**

Representative assignments in this course may include, but are not limited to the following:

Writing Assignments:

Students will be assigned weekly homework problems from the required textbook. Approximately four extensive analysis projects will be assigned which require problem solving and critical thinking. Students will write a report for each project. Students also will create and deliver presentations.

Reading Assignments:

Students will read all chapters of the required textbook, readings parallel current assignments, and lecture content. Extensive web searching is critical.

Other Outside Assignments:

Weekly homework problems, internet research, and working on presentations.

9. **REPRESENTATIVE METHODS OF EVALUATION**

Representative methods of evaluation may include:
    A. Class Participation
    B. Class Performance
    C. Class Work
    D. Exams/Tests
    E. Group Projects
    F. Homework
    G. Projects
    H. Quizzes
    I. Research Projects

10. **REPRESENTATIVE TEXT(S):**

Possible textbooks include:
    A. Williams, Barry. *Information Security Policy Development for Compliance*, ed. Auerbach Publications, 2013
    B. kim, David. *Fundamentals of Information Systems Security*, 3 ed. Jones & Bartlett Learning, 2016

Origination Date: March 2017
Curriculum Committee Approval Date: September 2018
Effective Term: Fall 2019
Course Originator: Kamran Eftekhari