

6. **Student Learning Outcomes** (Identify 1-6 expected learner outcomes using active verbs.)

Upon successful completion of the course, the student will be able to:

1. Analyze a client's company model and processes
2. Analyze a client's management model
3. Design an appropriate security solution for client organization
4. Evaluate the impact of a security design
5. Design remote services and DNS/SNMP security
6. Assess the network security risks and provide a plan for secure communication channels

7. **Course Objectives** (Identify specific teaching objectives detailing course content and activities. *For some courses, the course objectives will be the same as the student learning outcomes. If this is the case, please simply indicate this in this section).*

See Student Learning Outcomes

8. **Course Content** (Brief but complete topical outline of the course that includes major subject areas [1-2 pages]. Should reflect all course objectives listed above. In addition, you may attach a sample course syllabus with a timeline.)

See attached topical outline.

9. **Representative Instructional Methods** (Describe instructor-initiated teaching strategies that will assist students in meeting course objectives. Include examples of out-of-class assignments, required reading and writing assignments, and methods for teaching critical thinking skills.)

Course may include the following instructional methods as deemed appropriate by instructor:

Lecture to introduce new topics;

Instructor models problem-solving techniques;

Students participate in short in-class projects (in teacher-organized small groups) to ensure that students experiment with the new topics in realistic problem settings;

Teacher invites questions and answers from students, generating discussion about unclear areas;

Students work in small groups to solve significant networking problems;

10. **Representative Methods of Evaluation** (Describe measurement of student progress toward course objectives. Courses with required writing component and/or problem-solving emphasis must reflect critical thinking component. If skills class, then applied skills.)

Bi-weekly quizzes to provide feedback to students and teacher.

Observance of student contributions during discussion/project time,

Individual assignments involving network security design problems,

Midterm and Final exams (Short answer (textbook material) and problem solving (similar to inclass work))

Group participation on course projects, including peer-assessment of participation and contribution to the group effort.

11. **Representative Text Materials** (With few exceptions, texts need to be current. Include publication dates.)

Chiampa, Security+ Guide to Networking Security Fundamentals, 2ed, Course Technology, 2004

Campbell, Security+ Guide to Network Security Fundamentals, Course Technology, 2002

Prepared by:

(Signature)

Email address:

Submission Date: _____

CIS 479 - Network Security Fundamentals

Topical Outline

- I. Analysis
 - Analyzing the Company Model and Processes
 - Analyzing the Business Plan
 - Analyzing the Management Model
- II. Enterprise Risk Assessment
- III. Technology Review
- IV. Security Design Considerations
 - Evaluating the Impact of the Security Design on the Technical Environment
 - Security Baselines
- V. Designing the Security Solution
- VI. Authentication Strategy
 - Choosing an Authentication Strategy
 - Integration and Authentication Strategy
- VII. Enhancing Security Using Public Keys
- VIII. Building a DNS/SNMP Security Solution
- IX. Designing Remote Services Security
- X. Providing Secure Access at the Network Layer
- XI. Securing Communication Channels