Course Syllabus

**Department:** Computing Sciences

**Date:** 9/19/2012

I. **Course Prefix and Number:** CSC 275

   **Course Name:** Preparing for Security+ Certification

   **Credit Hours and Contact Hours:** 2 credit hours – 2 contact hours

   **Catalog Description including pre- and co-requisites:**

   Upon completion of the course the participant will be able to successfully complete the requirements for the Computing Technology Industry Association (CompTIA) Security+ Certification. The Security+ certification is an internationally recognized validation of the technical knowledge required of foundation-level security practitioners. A Security+ certified individual has successfully proven that he/she has acquired a foundation-level of skill and knowledge in general security concepts, communication security, infrastructure security, and understands the basics of cryptography and operational / organizational security.

   **Prerequisite:** students must be in the last semester of the AAS Information Technology degree program, the Networking and Security advisement area or have equivalent experience.

   **Relationship to Academic Programs and Curriculum including SUNY Gen Ed designation if applicable:**

   This course is offered as an elective in the AAS Information Technology degree, the Networking and Security advisement area.

II. **Course Student Learning Outcomes:**

   **Learning Outcomes**

   Upon completion of the course the participant should be prepared to take the Computing Technology Industry Association (CompTIA) Security+ Certification exam.

   **College Learning Outcomes Addressed by the Course:** (check each College Learning Outcome addressed by the Student Learning Outcomes)

   - [x] computer literacy
   - [ ] writing
   - [ ] oral communications
   - [ ] ethics/values
   - [ ] reading
   - [ ] citizenship
III. Assessment Measures (Summarize how the college and student learning outcomes will be assessed): For each identified outcome checked, please provide the specific assessment measure.

<table>
<thead>
<tr>
<th>List identified College Learning Outcomes(s)</th>
<th>Specific assessment measure(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>computer literacy</td>
<td><strong>Practice Problems:</strong> Students will complete practice Security+ exams given in years past, demonstrating a high level of computer security literacy.</td>
</tr>
<tr>
<td>critical thinking, information resources</td>
<td><strong>In-Class Quizzes:</strong> Students will complete regular in-class quizzes demonstrating well-reasoned arguments and critical thinking skills, and use appropriate information resources as they relate to course content.</td>
</tr>
</tbody>
</table>

IV. Instructional Materials and Methods

**Types of Course Materials:**
- Textbooks: a review, practice and case study book on Security+ Certification

**Methods of Instruction (e.g. Lecture, Lab, Seminar …):**
- Lecture
- Discussions
- Demonstrations

V. General Outline of Topics Covered:
The following is an examination blueprint outlining the knowledge domains covered by the Security+ Certification program. These will be the focus of the course.

**Core Knowledge Domains**
1. General Security Concepts 30%
2. Communication Security 20%
3. Infrastructure Security 20%
4. Basics of Cryptography 15%
5. Operational / Organizational Security 15%