# 8/15/2020

# brcc keystone logo

Baton Rouge Community College

*Academic Affairs Master Syllabus*

Date Approved: 2 September 2020

Term and Year of Implementation: Fall 2020

**Course Title:** PC and Network Security

**BRCC Course Rubric:** CNET 2503

**Previous Course Rubric**: CNET 250

**Lecture Hours per week-Lab Hours per week-Credit Hours**: 3-0-3

**Per semester: Lecture Hours-Lab Hours-Instructional Contact Hours**: 45-0-45

**Louisiana Common Course Number:**

**CIP Code:** 11.1003

**Course Description:** Provides an introduction in basic computer and network security skills, which includes developing a comprehensive approach to information security that embraces both the human and technical dimensions. Introduces fundamental concepts and principles of network security’s role, design, threats, policies, and elements of cryptography. Examines protocols, architectures, and technologies for secure systems and services.

**Prerequisites:**  None

**Co-requisites:** None

**Suggested Enrollment Cap:** 25

**Learning Outcomes.** *Upon successful completion of this course, the students will be able to:*

1. Implement fundamental features and infrastructure of system security.

2. Identify types of threats and methods for use to combat security issues.

3. Utilize various system audits and security tools.

4. Implement security plan that aligns with risk management procedures.

5. Describe the fundamentals of cryptography including Public Key Infrastructure.

**Assessment Measures.** Assessment of all learning outcomes will be measured using the following methods:

1. Structured use of class time

2. Instructor-prepared tests

3. Individual/Group Projects

4. Homework Assignments

**Information to be included on the Instructor’s Course Syllabi:**

* ***Disability Statement*:** Baton Rouge Community College seeks to meet the needs of its students in many ways. See the Office of Disability Services to receive suggestions for disability statements that should be included in each syllabus.
* ***Grading:*** The College grading policy should be included in the course syllabus. Any special practices should also go here. This should include the instructor’s and/or the department’s policy for make-up work. For example in a speech course, “Speeches not given on due date will receive no grade higher than a sixty” or “Make-up work will not be accepted after the last day of class”.
* ***Attendance Policy*:** Include the overall attendance policy of the college. Instructors may want to add additional information in individual syllabi to meet the needs of their courses.
* ***General Policies*:** Instructors’ policy on the use of things such as beepers and cell phones and/or hand held programmable calculators should be covered in this section.
* ***Cheating and Plagiarism*:** This must be included in all syllabi and should include the penalties for incidents in a given class. Students should have a clear idea of what constitutes cheating in a given course.
* ***Safety Concerns:*** In some courses, this may be a major issue. For example, “No student will be allowed in the lab without safety glasses”. General statements such as, “Items that may be harmful to one’s self or others should not be brought to class”.
* ***Library/ Learning Resources:*** Since the development of the total person is part of our mission, assignments in the library and/or the Learning Resources Center should be included to assist students in enhancing skills and in using resources. Students should be encouraged to use the library for reading enjoyment as part of lifelong learning.

**Expanded Course Outline:**

1. Basic Computer and Network Security Concepts and Principles
2. Legal and Privacy Issues
3. Internal Threats – Employees, Contractors, Third parties
4. External Threats – Criminals, Corporate Espionage, Hackers, Cyber Warfare, Cyber Terrorism
5. Cryptography
6. Secure Network Protocols
7. Access Control Models
8. Network Security Policies
9. Principles of Design
10. Social Engineering
11. Malware and viruses
12. Denial of Service Attacks and Defense
13. Penetration Testing, Vulnerability Scanning, and Security Auditing