Bossier Parish Community College
Master Syllabus

**Course Prefix and Number:** CTEC 287 **Credit Hours:** 3-3-0

**Course Title:** Network Security Design

**Course Prerequisites:** CTEC 155

**Textbook(s):** Prowse, David L. MindTap Information Security, 1 term (6 months) Instant Access for Ciampa's CompTIA Security+ Guide to Network Security Fundamentals, 6th Edition. Cengage. ISBN: 9781337289313.

**Software:** This course will use MindTap which helps prepare for the Security+ Certification.

**Course Description:** An introduction to fundamentals on designing, planning, and executing vulnerability analysis of networks. Students will work on multiple topics to include, but not limited to: System Security, Network Infrastructure, Access Control, Assessments & Audits, Cryptography, and organizational Security. This course is mapped to the CompTIA Security+ Exam. This course is a required course for earning CNSS 4011-4016 certifications.

**Learning Outcomes:**
At the end of this course, the student will:

A. recognize the basics of System Security;
B. identify Network Infrastructure;
C. recognize the fundamentals of Access Control;
D. conduct assessments and audits of systems;
E. implement basic Cryptography Skills; and
F. implement basic Organizational Security Skills.

To achieve the learning outcomes, the students will be able to:
(The letter designations at the end of each statement refer to the learning outcome(s).)

1. differentiate among various systems security threats (A);
2. implement OS hardening practices and procedures to achieve workstation and server security (A);
3. perform the appropriate procedures to establish application security (A);
4. explain the purpose and application of virtualization technology (A);
5. differentiate between the different ports and protocols, their respective threats and mitigation techniques (B);
6. determine the appropriate use of network security tools to facilitate network security (B);
7. apply the appropriate network tools to facilitate network security tools to facilitate network security (B);
8. explain the vulnerabilities and implement mitigations associated with wireless networking and various transmission media (B);
9. identify and apply industry best practices for access control methods (C);

10. organize users and computers into appropriate security groups and roles while distinguishing between appropriate rights and privileges (C);
11. deploy various authentication models and identify the components of each (C);
12. explain the difference between identification and authentication (ID Spoofing) (C);
13. conduct risk assessments and implement risk mitigation (D);
14. perform vulnerability assessments using common tools (D);
15. use monitoring tools on systems and networks and detect security-related anomalies (D);
16. conduct periodic audits of system security settings (D);
17. explain general cryptography, hashing and encryption concepts (E);
18. explain and implement protocols (E);
19. explain and implement PKI (E);
20. explain redundancy planning and its components (F);
21. implement disaster recovery procedures (F);
22. differentiate between and execute appropriate incident response procedures (F);
23. explain the importance of environmental controls (F);
24. identify and explain applicable legislation and organizational policies (F);
25. explain the concept of and how to reduce the risk of social engineering (F);
26. recognize INFOSEC security basics including: computer security and audit (A, D);
27. identify the NSTISS basics countermeasures including: technical surveillance countermeasures (C, F);
28. memorize the definition of manual/automated access controls (B);
29. recognize the importance of manual/automated access controls (B);
30. identify systems certifiers and accreditors in risk mitigation (D);
31. recognize the role of Information Assurance Manager (ISSM) (D); and
32. recognize the role of System Security Officer (ISSO) (D).

**Course Requirements:**

1. The certification exam(s) for this course is required to be taken on campus or an approved proctored environment.
2. A student must successfully complete the course with an average of 70% or above on the combined learning outcomes.
3. Each student is expected to attend classes regularly; excessive unexcused absences constitute grounds for suspension (refer to the student handbook for attendance policies).

**Course Grading Scale:**

A = 90 - 100
B = 80 - 89
C = 70 - 79
D = 60 - 69
F = 0 - 59

**Attendance Policy**: The college attendance policy is available at http://www.bpcc.edu/catalog/current/academicpolicies.html

**Course Fees:** This course is accompanied with an additional non-refundable fee for supplemental materials, laboratory supplies, software licenses, certification exams and/or clinical fees.

**Nondiscrimination Statement:** Bossier Parish Community College does not discriminate on the basis of race, color, national origin, gender, age, religion, qualified disability, marital status, veteran's status, or sexual orientation in admission to its programs, services, or activities, in access to them, in treatment of individuals, or in any aspect of its operations. Bossier Parish Community College does not discriminate in its hiring or employment practices.

COORDINATOR FOR SECTION 504 AND ADA
Angie Cao, Student and Disability Services Specialist
Disability Services, F-254
6220 East Texas Street
Bossier City, LA 71111
Phone: 318-678-6511
Email: acao@bpcc.edu
Hours: 8:00 a.m.-4:30 p.m. Monday - Friday, excluding holidays and weekends.

Equity/Compliance Coordinator
Teri Bashara, Director of Human Resources
Human Resources Office, A-105
6220 East Texas Street
Bossier City, LA 71111
Phone: 318-678-6056
Hours: 8:00 a.m.-4:30 p.m. Monday - Friday, excluding holidays and weekends.