Bossier Parish Community College
Master Syllabus

Course Prefix and Number: CTEC 279 **Credit Hours:** 3-3-0

Course Title: Information Assurance

Course Prerequisites: None

Textbook(s): Mindtap Information Security, 1 term (6 months) Instant Access for Michael Whitman. Principles of Information Security, 6th edition. Cengage.
ISBN: 9781337281645.

Software: Mindtap

Course Description: This course is an introduction to the field of Information Assurance (Security). Various kinds of threats that might be faced by an information system and the security techniques used to fight them are covered. Hacker methods, viruses, worms, bombs, and system vulnerabilities are described with respect to the actions that must be taken by a Network Manager to thwart them. Existing and planned protection methods and defenses are mapped to the information system threats and attacks. This course provides the background for those individuals who seek skills in the areas of Network and Data Security. This course also is part of the courses required to get CNSS 4011 - 4016 certifications.

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

A. apply general security elements;
B. interpret network security issues;
C. interpret system security issues; and
D. implement security assurance.

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

1. define Information Security (A);
2. describe threats to IT assets, security process and encryption methods (A);
3. recognize the fundamentals of network security (B);
4. identify network security threats (B);
5. use UNIX system security (C);
6. use Windows system security (C);
7. identify legal, ethical, and professional issues in IA (A,B,C,D);
8. recognize the standards and compliance for IA (D);
9. execute security testing (D);
10. recognize security basics operations security including: OPSEC interdependency, OPSEC process, OPSEC surveys/OPSEC planning and unclassified indicators (A);

11. identify NSTISS basics threats to vulnerabilities of systems including: threat impact areas (A, B);
12. implement NSTISS basics countermeasures including: monitoring (e.g., data, line) (B, D);
13. identify NSTISS basics concepts of risk management and planning and management of risk management including: monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information), threat and vulnerability assessment, acceptance of risk (accreditation), corrective actions, information identification, risk analysis and/or vulnerability assessment components, risk analysis results evaluation, and roles and responsibilities of all the players in the risk analysis process (A, D);
14. recognize NSTISS basics Concepts of System Life Cycle Management and planning and management of system life cycle management including: demonstration and validation (testing), development, implementation, requirements definition (e.g., architecture), security (e.g., certification and accreditation), acquisition, design review and systems test performance (ensure required safeguards are operationally adequate) and management control process (ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications) (A, C, D);
15. identify NSTISS basics concepts of trust including: assurance, mechanism and policy (D);
16. recognize NSTISS basics roles of various organizational personnel including: audit office, COMSEC custodian, end users, information resources management staff, INFOSEC officer, OPSEC managers, program or functional managers, security office, senior management, system manager and system staff and telecommunications office and staff (D);
17. recognize the NSTISS basics facets of NSTISS including protection of areas, protection of data communications, protection of equipment and reporting of security violations (A, D);
18. learn the NSTISS policies and procedures of software security including: configuration management (change controls), configuration management (documentation), configuration management (programming standards and controls), software security mechanisms to protect information: access privileges, application security features, audit trails and logging, concept of least privilege, identification and authentication, and segregation of duties (C);
19. explain the importance of SSM Role in Information Assurance (A,C);
20. discuss and explain the importance of accreditation (A,D);
21. discuss and explain the importance of threats and attacks to the system (C,D);
22. discuss and explain threats, threat analysis and assessment (D);
23. explain the importance of educational training and awareness as countermeasures (D);
24. explain the importance of countermeasures (D);
25. explain the importance of vulnerability analysis, importance of network and technical vulnerabilities (A,B);
26. explain the importance of cost/benefit analysis of information assurance (D);
27. discuss and Explain types risk, risk analysis, and risk assessment (A);
28. explain the importance of access control policies (B);

29. explain the importance of administrative security, audit, logging, documentation policies/procedures (A,B);
30. explain authentication (A);
31. explain the importance of background investigations (A);
32. explain the importance of business recovery (A);
33. explain the importance of contingency/continuity of operations planning (A); and
34. explain the importance of disaster and recover recovery planning as well as incident response (A,D).

Course Requirements:

1. A student must successfully complete the course with an average of 70% or above on the combined learning outcomes.
2. 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.