Bossier Parish Community College
Master Syllabus

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

Course Title: Information Assurance

Course Prerequisites: CTEC 112

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

Optional Textbook/Subscription Offers from Cengage:
Cengage Unlimited, 1 term (4 month) Printed Access Card, 1st edition,
PAC: 9780357700037 or IAC: 9780357700006
Cengage Unlimited, Multi-term (12 month) Printed Access Card, 1st edition,
PAC: 978035770044 or IAC: 9780357700013
Cengage Unlimited, Multi-term (24 month) Printed Access Card, 1st edition,
PAC: 9780357700051 or IAC: 9780357700020

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 is a required course for the NSA/DHS KU alignment for the CAE-CDE Designation.

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,B,C,D);
2. describe threats to IT assets, security process and encryption methods (A,D);
3. recognize the fundamentals of network security (B,D);
4. identify network security threats (B);
5. use operating system (OS) security (A,C);

6. identify legal, ethical, and professional issues in IA (A,B,C,D);
7. recognize the standards and compliance for IA (A,D);
8. execute security testing (A,D);
9. recognize security basics operations security including: OPSEC interdependency, OPSEC process, OPSEC surveys/OPSEC planning and unclassified indicators (A);
10. identify and discuss NSTISS basics concepts of risk management, planning and management of risk management including: monitoring the efficiency and effectiveness of controls, 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);
11. recognize 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);
12. identify basics concepts of trust including: assurance, mechanism and policy (A,B,C);
13. recognize 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);
14. learn the 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);
15. discuss and explain the importance of accreditation (A,D);
16. discuss and explain threats, threat analysis and assessment (C,D);
17. explain the importance of educational training and awareness as countermeasures (D);
18. explain the importance of countermeasures (B,D);
19. explain the importance of vulnerability analysis, importance of network and technical vulnerabilities (A,B);
20. explain the importance of cost/benefit analysis of information assurance (D);
21. explain the importance of access control policies (B,D);
22. explain the importance of administrative security, audit, logging, documentation policies/procedures (A,B);
23. explain authentication (A);
24. explain the importance of background investigations (A);
25. explain the importance of business recovery (A);
26. explain the importance of contingency/continuity of operations planning (A);

27. explain the importance of disaster and recover recovery planning as well as incident response (A,D);
28. Explain basic principles of cryptography (A,B); and Explain basic roles of IDS/IPS (A,B,C).

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://catalog.bpcc.edu/content.php?catoid=5&navoid=369

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.

Vocabulary: Advanced persistent threat, attacker, block cipher, DoS, DDoS, malware, mitigations, residual risk, risk, stream cipher, vulnerability, BYOD, IaaS, PassS, SaaS, SAN, USB,

NICE Framework Categories:

Securely Provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)
Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)
Investigate (IN)		

Specializations:

- Data Management Systems Security
- Data Security Analysis
- Digital Forensics
- Cyber Investigations
- Health Care Security
- Industrial Control Systems – SCADA Security
- Network Security Administration
- Network Security Engineering
- Security Incident Analysis and Response
- Security Policy Development and Compliance

- Systems Security Engineering
- System Security Administration
- Secure Cloud Computing
- Secure Embedded Systems
- Secure Mobile Technology
- Secure Telecommunications

CAE Knowledge Unit Mapping:

- Cybersecurity Foundations (CSF)
- IT Systems Components (ISC)
- Basic Cryptography (BCY)
- Network Defense (NDF)
- Cybersecurity Planning and Management (CPM)
- Policy, Legal, Ethics, and Compliance (PLE)
- Security Risk Analysis (SRA)
- IA Standards (IAS)
- Network Security Administration (NSA)
- Vulnerability Analysis (VLA)

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.