Big Bend
COMMUNITY COLLEGE

MASTER COURSE OUTLINE
Prepared By: Mary Shannon   Date: January 2015

COURSE TITLE
Introduction to Security Administration

GENERAL COURSE INFORMATION
Dept.: CS   Course Num: 207   (Formerly:)
CIP Code: 11.0901   Intent Code: 21   Program Code: 527
Credits: 5
Total Contact Hrs Per Qtr.: 55
Lecture Hrs: 55   Lab Hrs: Other Hrs:
Distribution Designation: General Elective (GE)

COURSE DESCRIPTION (as it will appear in the catalog)
This course builds on prior course work in computer hardware, operating systems, and networks. Students will acquire the specific skills required to implement basic security services on any type of computer network and be prepared to take the CompTIA Security+ exam.

PREREQUISITES
CS 105 and CS 110, or Instructor Permission

TEXTBOOK GUIDELINES
Textbook and materials to be determined by CS Faculty (Example: *Introduction to Computer Security)*

COURSE LEARNING OUTCOMES
Upon successful completion of the course, students should be able to demonstrate the following knowledge or skills:

1. Identify fundamental concepts of computer security
2. Identify security threats
3. Harden internal systems and services
4. Harden internetwork devices and services
5. Secure network communications
6. Manage Public-Key Infrastructure (PKI)
7. Manage certificates
8. Enforce organizational security policies
9. Monitor the security infrastructure

INSTITUTIONAL OUTCOMES

COURSE CONTENT OUTLINE

1. Computer Security Overview
2. Cryptographic Tools
3. User Authentication
4. Access Control

5. Database Security
6. Malicious Software
7. Denial-of-Service Attacks
8. Intrusion Detection
9. Firewalls and Intrusion Prevention Systems
10. Buffer Overflow
11. Software Development Security
12. Operating System Security
13. Trusted Computing and Multilevel Security
14. IT Security Management and Risk Assessment
15. IT Security Controls, Plans, and Procedures
16. Physical and Infrastructure Security
17. Human Resources Security
18. Security Auditing
19. Legal and Ethical Aspects
20. Symmetric Encryption and Message Confidentiality
21. Public-Key Cryptography and Message Authentication
22. Internet Security Protocols and Standards
23. Internet Authentication Applications
24. Wireless Network Security

DEPARTMENTAL GUIDELINES *(optional)*

___________________________________ __________________

DIVISION CHAIR APPROVAL **DATE**