GROSSMONT COLLEGE

 Official Course Outline

COMPUTER SCIENCE INFORMATION SYSTEMS 121 – INTRODUCTION TO CYBERSECURITY

 1. Course Number Course Title Semester Units Semester Hours

 CSIS 121 Introduction to 3 2 hours lecture: 32-36 hours

 Cybersecurity 3 hours lab: 48-54 hours

 64-72 outside-of-class hours

 144-162 total hours

 2. Course Prerequisites

 None.

 Corequisite

 None

 Recommended Preparation

 None.

 3. Catalog Description

 Practical introductory course intended for those interested in learning about cybersecurity. Lectures, laboratories, and practical assignments will emphasize skills needed to work effectively in the area of cybersecurity. Some topics include: Internet security basics, hackers, spyware, phishing, spam, zombies, Trojan horses, worms, viruses, wi-fi security, denial-of-service, web-blocking, firewalls, and proxy servers, operating system security, browser and web security, and cryptography. Includes installation and configuration of security tools and utilities.

 4. Course Objectives

Students will:

1. Describe how the Internet works in relationship to cybersecurity.
2. Differentiate between various types of hackers and hacking techniques.
3. Identify spyware, phishing, and spam and analyze tools to defeat them.
4. Identify malware such as Trojan horses, zombies, worms, and viruses.
5. Explain denial-of-service threats and configure firewalls and proxy servers.
6. Harden operating systems with security and enhance browser and web security.
7. Analyze Wi-Fi security threats and implement cryptography techniques.
8. Install and configure security tools and utilities.

 5. Instructional Facilities

 Computer equipped classroom with Internet access and appropriate software and hardware.

 6. Special Materials Required of Student

1. File storage system
2. Access to web-based course material

COMPUTER SCIENCE INFORMATION SYSTEMS 121 – INTRODUCTION TO CYBERSECURITY Page 2

 7. Course Content

1. TCP/IP
2. Client/server model
3. Basic networking protocols
4. How hackers invade PCs and networks
5. Spyware and anti-spyware
6. Phishing and spam
7. Zombies and Trojan horses
8. Worms, viruses, and malware
9. Wi-Fi security threats
10. Denial-of-service threats
11. Firewalls and proxy servers
12. Operating Systems security
13. Browser and web security
14. Cryptography

8. Method of Instruction

1. Lecture and demonstration
2. Hands-on practice
3. Assignments

 9. Methods of Evaluating Student Performance

1. Quizzes and exams including a final that measure students’ ability to use cybersecurity terminology and to explain cybersecurity concepts.
2. Practical exams that measure students’ ability to use cybersecurity knowledge and skills to demonstrate proficiency in cybersecurity components.
3. Projects that measure students’ ability to conceptualize and apply cybersecurity concepts.
4. Exercises that measure students’ ability to identify cybersecurity concerns and to address those concerns with practical solutions.

10. Outside Class Assignments

1. Assign textbook reading.
2. Complete assignments, labs, and online quizzes identifying network threats in a business environment.
3. Review online resources, including videos.

d. Analyze compromised systems to identify and resolve security threats.

11. Textbook(s)

Required Textbook(s):

 Conklin, W. and G. White. *Principles of Computer Security.* (Official Comptia Guide) 4th ed., New York, NY: McGraw-Hill, 2016.

 Addendum: Student Learning Outcomes

 Upon completion of this course, our students will be able to do the following:

1. Recognize signs of typical Cybersecurity breaches in order to be able to define the issues and challenges in addressing them.
2. Apply best practices in problem analysis needed to implement effective and efficient Cybersecurity solutions.
3. Demonstrate the capability to implement an appropriate solution to solve the Cybersecurity challenge.

Date approved by the Governing Board: May 15, 2018