HOSTOS COMMUNITY COLLEGE
DEPARTMENT OF MATHEMATICS
AND COMPUTER SCIENCE

CST 240: INTRODUCTION TO CYBERSECURITY

Credit Hours: 3.0

Lab Hours: 2.0

Class Hours: 2.0

Prerequisite: CST 220

Course Description:

This course is an introduction to security issues facing computer professionals today. Students will acquire the knowledge and skills on how to maintain the integrity, authenticity, availability, and privacy of data. It covers computer viruses, authentication models, certificates; group policy, cryptography, and access control. It also introduces the fundamental security issues of programming, database, and web server. Other topics include how to monitor the system for suspicious activity and fend off attacks, to keep spies and Spam out of the e-mail, to take control of security by encrypting data, to design an active directory, blocking ports, and locking down the registry.

Required Text:

M. Whitman and H. Mattord, Principles of Information Security, 7th Ed.,

ISBN-10: 035750643X

ISBN-13: 978-0357506431

Grades: A, A$^-$, B$^+$, B, B$^-$, C$^+$, C, D, F

Objective: This is the first course of the information security module. It equips students and computing professionals with the basic information security knowledge and operating system security skills needed to implement and maintain modern information infrastructure and systems.

Learning Outcomes:

At the end of the course, students should be able to:

- Demonstrate an understanding of the risks and vulnerabilities associated with computer programs.
- Maintain the integrity, authenticity, availability, and privacy of data.

- Demonstrate an understanding of how to protect privacy by using cryptography.
- Demonstrate an understanding of network protocols and the risks and vulnerabilities associated with computer networks.
- Demonstrate an understanding of the risks and vulnerabilities associated with operating systems.
- Secure the Windows and LINUX/UNIX operating systems.

Student Learning Outcomes:

1. Students will demonstrate proficiency in defining risk management and discuss the stages in the risk management process.
2. Students will be able to understand external and internal information security threats to an organization.
3. Students will demonstrate fluency in developing the process of information security policies and guidelines.
4. Students will demonstrate fluency with policy structures, guidelines, standards, security awareness, and their importance.
5. Students will demonstrate proficiency in discovering, analyzing, and dealing with threats.

Topics and Schedule:

Part I: Introduction to Information Security Issues

Week 1: Introduction to Information Security

Week 2: The Need for Security

Weeks 3-4: Legal, Ethical, and Professional Issues in Information Security.

Weeks 5-6: Risk Management, Physical Security

Week 7: Midterm

Part II: Introduction to Cryptography and Operating System Security)

Weeks 8-9: Cryptography I

Weeks 10-11: Public Key Cryptography (RSA and Diffie-Hellman Algorithm)

Weeks 12-13: Planning for Security

Week 14: Selective Security Topics (e.g. Microsoft Windows Server 2008, Cloud security)

Week 15: Project presentation & FINAL