RARITAN VALLEY COMMUNITY COLLEGE
COURSE OUTLINE

CISY 229 – Information Security Fundamentals

I. Basic Course Information

A. Course Number & Title: CISY-229 – Information Security Fundamentals

B. New or Modified Course: Modified

C. Date of Proposal: Semester: Fall Year: 2016

D. Effective Term: Fall 2017

E. Sponsoring Department: Computer Science

F. Semester Credit Hours: 3

G. Weekly Contact Hours:
Lecture: 3
Laboratory:
Out of class student work per week: 6

H. Prerequisite: CISY 119 Networking Essentials or
CISY 270 Introduction to Cisco Networking

I. Laboratory Fees: No

J. Name and Telephone Number or E-Mail Address of Department Chair at time of approval: Steven Schwarz, steven.schwarz@raritanval.edu

II. Catalog Description

<u>*Prerequisite:*</u> *CISY 119 Networking Essentials or CISY 270 Introduction to Cisco Networking.* This course introduces the student to fundamental computer and network security concepts. These concepts are presented using the framework of the CISSP (Certified Information Systems Security Professional) ten domains of security which will help prepare the student for the CISSP certification examination. This course introduces students to the application of information security principles in supporting IT architectures, management and data protection. Students learn to design and implement security solutions which balance the demands of technology, processes, policies, budgets, and the workplace environment.

III. Statement of Course Need

A. Due to the widespread acceptance of both networking and Internet integration in most all business models and widespread personal use of high-speed internet access and home networks, many computers are vulnerable to a wide range of malicious attacks. The widespread knowledge of this vulnerability, the low threshold of knowledge needed to exploit many of the vulnerabilities, and the funding and/or use of such attacks by many countries and special interest groups as "information warfare", has created a need for comprehensive security measures to be administrated on all networks. This need is being recognized by many small to medium sized businesses that until now have not had security policies. The increase in companies of all sizes which now are engaged in web based information transfers, such as e-business, data mining, and product information distribution, has created a large market for security professionals. In addition to the financial risks that security breaches cause, new Federal and European Union laws requiring stringent privacy requirements have created legal risks for companies with poor data security.

B. This course does not have a Lab component

C. This course generally transfers as a Computer Science Elective

IV. Place of Course in College Curriculum

A. Free Elective
B. This course meets a program requirement for:
    a. Computer Networking and Security Certificate
    b. Computer Networking AAS
C. This course meets a program option for:
    a. Information Systems & Technology AAS
D. CIS Elective from the Computer Science (CISY) Electives List
E. Course Transferability: for New Jersey schools go to the NJ Transfer website, www.njtransfer.org . For all other colleges and universities, go to their individual websites

V. Outline of Course Content

A. Introduction to Information Security and the 10 domain structure of the CISSP, and future directions in the field.

B. Security Architecture & Models
    1. Security Architecture & Models defined.
    2. Modes of attack available at each level of the Security Architecture

C. Telecommunications & Network Security
    1. Network low level vulnerabilities & communication interception
    2. Firewall software - levels at which it can monitor activity and deny access

D. Access Control Methods
   1. Methods of breaking access controls (hacking)
   2. Quality of workplace and privacy issues related to biometric and other personal information

E. Application and Systems Development
   1. The role of security throughout the Software Life Cycle Development Process
   2. Security needs for Common application types
   3. Application and systems vulnerabilities

F. Operations Security
   1. Security measures in System Administration (controls, protections, monitoring, and auditing)
   2. Anti-virus software operation and functionality

G. Cryptography Basics and Vulnerabilities

H. Business Continuity Planning and Disaster Recovery Planning

I. Law, Investigation, Ethics and Forensics

J. Physical Security threats and vulnerabilities

K. Security Management Practices
   1. Security Policies and Information Classification
   2. Roles, Responsibilities, and Risk Management

VI. General Educational and Course Learning Outcomes

A. <u>General Educational Learning Outcomes</u>

At the conclusion of the course, students will be able to:

1. Use the Internet for research, information analysis, problem solving, and decision making regarding information security and present their findings (GE-NJ 1, IL).

2. Recognize ethical and legal issues as they pertain to security measures, information handling, and other workplace events (GE-NJ ER)

B. Course Learning Outcomes

Upon completion of this course, students will be able to:

1. Explain the 10 domains of computer security
2. Evaluate the types of vulnerabilities a system may have and which level of networking may be affected by them
3. Design a corporate information security strategy addressing the major information security principles
4. Design and implement a Business Continuity and Disaster Recovery Plan
5. Research appropriate resources regarding legal and ethical issues, business needs, software upgrades, and vulnerabilities (Goal 2)
6. Research on relevant information security topics and present findings (Goal 1)

C. Assessment Instruments

1. Weekly homework assignments
2. Research papers
3. Oral presentations
4. Exams and quizzes
5. Mid-term and final exams
6. Classroom (or online forum) participation

VII. Grade Determinants

A. Essays
B. Projects – to include either Corporate Security Plan and/or Corporate Backup and Disaster Recovery Plan
C. Exams
D. Oral Presentations

Methods of teaching and learning that may be used in the course:
A. lecture/discussion (may be online)
B. small-group work
C. student oral presentations
D. simulation/role playing

VIII. Texts and Materials

Suggested Textbook – *Official (ISC)^2 Guide to the CISSP CBK, Fourth Edition*, Gordon, Adam, ((ISC)^2 Press), 2015

(Please Note: The course outline is intended only as a guide to course content and resources. Do not purchase textbooks based on this outline. The RVCC Bookstore is the sole resource for the most up-to-date information about textbooks.)

IX. Resources

A. standard library resources
B. video projection equipment