RARITAN VALLEY COMMUNITY COLLEGE
ACADEMIC COURSE OUTLINE

NTWK 229 Information Security Fundamentals

I. Basic Course Information

A. Course Number and Title: NTWK 229 Information Security Fundamentals

B. New or Modified Course: Modified

C. Date of Proposal: Semester: Fall Year: 2024

D. Effective Term: Fall 2025

E. Sponsoring Department: Math & Computer Science

F. Semester Credit Hours**:** 3

G. Weekly Contact Hours**:** 4 Lecture**:** 2
Laboratory**:** 2
Out of class student work per week: 5

H. ☐ Prerequisite (s):
☐ Corequisite (s):

I. Additional Fees**:** None

II. Catalog Description

(Prerequisites: None) This course is based on the industry performance-based COMPTIA Security+ certification. It focuses on the latest trends and techniques in risk management, risk mitigation, threat management and intrusion detection. Security+ is compliant with ISO 17024 and approved by the US DoD to meet directive 8140/8570.01-M requirements.

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 dependent on the institution.

IV. Place of Course in College Curriculum

A. Free Elective

B. This course serves as a program requirement in:
   a. Computer Networking and Cybersecurity A.A.S.
   b. Computer Support Certificate
   c. Computer Networking and Cybersecurity Certificate

C. This course serves as a Computer Elective on the Computer and Programming Electives List.

D. To see course transferability: a) for New Jersey schools, go to the NJTransfer website, www.njtransfer.org; b) for other colleges and universities, go to the individual websites for those schools

V. Outline of Course Content

The outline for the course is below. This outline can be adapted by individual instructors according to the order in which they cover content.

A. Security Basics
   1. Understanding Attacks
   2. Defense Planning
   3. Access Control
   4. Cryptography Basics
   5. Network Monitoring
   6. Incident Response

B. Policies, Procedures, and Awareness

1. Security Policies
2. Risk Management
3. Business Continuity
4. Manageable Network Plan
5. Social Engineering
6. App Development and Deployment
7. Employee Management
8. Mobile Devices
9. Third-Party Integration

C. Physical

1. Physical threats
2. Device Protection
3. Network Infrastructure Protection
4. Environmental Controls

D. Perimeter

1. Recon and Denial
2. Spoofing and Poisoning
3. Security Appliances
4. Demilitarized Zones (DMZ)
5. Firewalls
6. Network Address Translation (NAT)
7. Virtual Private Networks (VPN)
8. Web Threat Protection
9. Network Access Protection
10. Wireless Overview
11. Wireless Attacks
12. Wireless Defenses

E. Network

1. Network Threats
2. Network Device Vulnerabilities
3. Network Applications
4. Switch Attacks
5. Switch Security
6. Using VLANs
7. Router Security
8. Intrusion Detection and Prevention
9. Vulnerability Assessment
10. Protocol Analyzers
11. Remote Access
12. Network Authentication
13. Penetration Testing

14. Virtual Networking
15. Software-Defined Networking (SDN)
16. Cloud Services

F. Host

1. Malware
2. Password Attacks
3. Windows Systems Hardening
4. Hardening Enforcement
5. File Server Security
6. Linux Host Security
7. Embedded Systems
8. Log Management
9. Audits
10. Email
11. BYOD Security
12. Mobile Device Management
13. Host Virtualization

G. Application

1. Access Control Models
2. Authentication
3. Authorization
4. Web Application Attacks
5. Internet Browsers
6. Application Development
7. Active Directory Overview
8. Windows Domain Users and Groups
9. Linus Users
10. Linux Groups
11. Linux User Security
12. Group Policy Overview
13. Hardening Authentication

H. Data

1. Data management
2. Advanced Cryptography
3. Cryptography Implementations
4. Cryptographic Attacks
5. Symmetric Encryption
6. Asymmetric Encryption
7. File Encryption
8. Public Key Infrastructure
9. Hashing
10. Data Transmission Security
11. Data Loss Prevention (DLP)

12. Redundancy
13. Backup and Restore
14. Cloud Storage

VI. A. Course Learning Outcomes

At the completion of this course, the student 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- 1, IL).
2. Describe use cases and purpose for frameworks, best practices and secure configuration guides (GE-1, 4)
3. Summarize basic concepts of forensics, business impact analysis and cloud and virtualization concepts (GE-1, 4)
4. Analyze the importance of policies, plans and procedures related to organizational security
5. Describe disaster recovery and continuity of operation concepts (GE-1)
6. Summarize secure application development and deployment concepts
7. Compare physical security and environmental controls and analyze the impact associated with types of vulnerabilities (GE-4*)
8. Explain the security implications of embedded systems, penetration testing and threat types and attributes (GE-1, 4)
9. Compare basic concepts of cryptography, access concepts and risk management
10. Explain disaster recovery and continuity of operation and how resiliency and automation strategies reduce risk (GE-1)

A. 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 for 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

A. Suggested Textbook

Suggested Textbook- COMPTIA Security+ Guide to Network Security Fundamentals, Sixth Edition, Mark Ciampa, Cengage Learning, 2018

Testout: Testout Security Pro

(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. Access to General Purpose Computers with Internet Access
B. The Library – for optional research projects
C. video projection equipment
D. Internet Access

X. Check One: ☐Honors Course ☐Honors Options ☒ N/A