RARITAN VALLEY COMMUNITY COLLEGE
ACADEMIC COURSE OUTLINE

NTWK 274 Privacy, Ethics & Computer Forensics

I. Basic Course Information

    A. Course Number and Title: NTWK 274 Privacy, Ethics & Computer Forensics

    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

(Prerequisite: none). This course provides the student with an understanding of security issues pertaining to privacy and ethics, as well as instruction and practice of forensics skills. Students perform hands-on exercises using the UNIX, Linux, and Windows operating system, including evidence collection and forensics activities at various levels including technical and process-oriented exercises. Students learn how to collect, catalog, sort, analyze and organize evidence. In addition, students learn how to package and present their findings to legal and law enforcement agencies with special consideration given to privacy issues and ethics.

III. Statement of Course Need

A. Due to the widespread acceptance of both networking and Internet integration into most business models, and widespread personal use of high-speed internet access and home networks, many computers are now 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 caused 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 a security policy.

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. Ethics, laws and privacy issues have become part of the fabric of conducting business over the internet. Therefore understanding citizen rights for privacy, ethical consideration for investigators and the limitation and boundaries of the law have all become interconnected in the new world of doing business over the internet.

B. This course does have lab component. Students are expected to use computers in the lab to work with various operating systems.

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
  d. Web Developer A.S.
  e. Web Developer 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. Introduction.
   1. Rationale for forensics, ethics, and privacy
   2. The role of security fits in the overall IT industry.
   3. Potential areas of employment

B. Risk mitigation
   1. Understanding damage control, crime in cyberspace, cyber terror, information warfare, hackers, crackers, and social engineering
   2. Motives, threats and trends
   3. Privacy issues and constitutional protections
   4. Legal issues regarding computer seizure
   5. Court references and dependencies

C. Incident response techniques, processes and architecture
   1. The need for Incident Response and Forensics
   2. Computer Intrusion Laws
   3. Incident response preparation and toolkits
   4. Incident verification and response actions
   5. Trend analysis and tracking incidences
   6. Raid and Seizure
   7. Evidence recording, photographing, backup, labeling, classifying and storage

D. Preservation of evidence
   1. Digital evidence
   2. Verifying without damaging evidence
   3. Escalation techniques
   4. Preserving the chain of evidence
   5. Contacting law enforcement agencies
   6. Coordinating with legal and understanding the law
   7. Detailing and logging the event
   8. Identify digital and non-digital artifacts.
   9. System and network logs
   10. Cost of damage including hours expended in incident recovery, loss of revenue, and value of trade secrets

E. Analysis of computer files based on file creation, file modification and file access

F. Mal-ware - understanding viruses, Trojan horses, worms, and bombs
   1. Abnormal Processes
   2. Reviewing Relevant Files
   3. Unusual or Hidden Files

4. Unauthorized Access Points
5. Trust Relationships
6. Security Identifiers

G. Differences among DOS, Windows and Windows NT/2000/XP from a forensics standpoint. Windows methods that will ensure maximum evidence capture.

H. Computer forensics processing methods and procedures
    1. Trust Relationships Forensics
    2. Incident handling
    3. Intellectual property theft, computer abuse, and intrusions,
    4. Investigative methods for incident response
    5. Documentation of computer forensics findings for use in trial and management review
    6. Issues relevant to overcoming a legal junk science attack.

I. Cyberspace Ethics
    1. Ethics in the new internet age
    2. Homeland security
    3. Social responsibilities
    4. Role of government in ethics
    5. Business responsibilities
    6. Personal responsibilities

J. Privacy Environment
    1. HIPAA, EU Directives, GLB, CPNI, PI, CA 1386
    2. Privacy assessment and policy
    3. Privacy incident reporting and tracking
    4. Acceptable use and acceptable terms

VI. A. <u>Course Learning Outcomes</u>

At the completion of this course, the student will be able to:

1. Communicate information security solutions that reflect critical and creative thought (GE-1*)
2. Use the Internet for research, information analysis, problem solving, and decision making regarding information security (GE-IL).
3. Develop the ability to make informed judgments concerning ethical issues in Information Security (GE-NJ 9)
4. Identify the types of security and privacy threats that are prevalent today. Categorize and identify the types of malicious software currently used to exploit these threats.
5. Perform a security evaluation and draft a security policy for an enterprise class or smaller entity. (GE-1)
6. Explain the legal constraints required by security and privacy related laws and regulations

as they pertain to information security and intrusion investigations. (GE-1)
7. Prepare and implement a procedure for responding to computer intrusions, including documentation of methods used, tracking of evidence, and other methodologies needed for the forensic investigation to pass legal challenges in court.
8. Explain the ethical issues involved in security practices at the governmental, business, and personal levels. (GE-1, ER)

B. <u>Assessment Instruments</u>

    a. laboratory products & reports
    b. weekly assignments
    c. research papers
    d. oral presentations
    e. exams and quizzes
    f. mid-term and final exams
    g. classroom participation

VII. Grade Determinants

A. Laboratory products & reports
B. Weekly assignments
C. Research paper
D. Oral presentations
E. Exams/quizzes

Methods for teaching and learning that may be used in the course:

A. lecture/discussion
B. small-group work
C. computer-assisted instruction
D. laboratory exercises
E. student oral presentations
    simulation/role playing

VIII. Texts and Materials

A. Suggested Textbook

Suggested Textbooks

1. Hacking Exposed by Joel Scambray, Stuart McClure and George Kurtz, McGraw-Hill Professional Publishing; ISBN: 0072127481

2. The CISSP Prep Guide: Mastering the Ten Domains of Computer Security by Ronald L. Krutz, Russell Dean Vines, Edward M. Stroz (Foreword), John Wiley & Sons; ISBN: 0471413569

(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

1. library resources
2. technology support
3. Hands-on Networking Lab (currently at Bridgewater, B105)
4. http://www.cissp.com/default.html, the web portal for the certified information systems security professional
5. http://www.microsoft.com

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