ROCHESTER COMMUNITY AND TECHNICAL COLLEGE

COMMON COURSE OUTLINE

Course discipline/number/title: COMP 2048: Introduction to Cybersecurity

A. CATALOG DESCRIPTION

1. **Credits: 4**
2. **Hours/Week: 4 hours per week lecture**
3. **Prerequisites (Course discipline/number):** COMP 1080, MATH 0099
4. **Other requirements:** None
5. **MnTC Goals (if any):** NA

B. COURSE DESCRIPTION: This class holistically examines cybersecurity processes and procedures, including assessment of the security posture of an organization, monitoring and securing an environment, operating within laws and guidelines, including compliance, risk assessment, and security governance, and identifying, analyzing, and responding to incidents. Focus is applied to proper security architecture, identifying threats, implementing mitigations, and incident response while working within the confines of governmental and global regulations, together with compliance standards. This class aligns to the CompTia Security+ exam.

C. DATE LAST REVISED (Month, year): November, 2023

D. OUTLINE OF MAJOR CONTENT AREAS:

1. Intro to Cybersecurity
   a) CIA Triad
   b) CompTia Security+ Exam Overview
   c) Stakeholders in Cybersecurity
   d) Career Prospects
2. Fundamentals of Security Architecture
   a) Security Architecture and Design
   b) Layered Security and Defense in Depth
3. Risk Assessment
   a) Key Terminology
   b) Conducting Risk Assessments
4. Implementing Security Controls
   a) Types of Security Controls
   b) Best Practices
5. Identification of Threat Vectors and Vulnerabilities
   a) Threat Vectors
   b) Vulnerability Assessment
6. Regulatory and Compliance Standards
   a) Compliance Standards
   b) Regulatory Standards
7. Types of Attacks and Defense Methods
   a) Common Attack Types
   b) Defense Methods
8. Threat Detection and Incident Response
   a) Threat Detection Methods
   b) Incident Response Procedures
9. Identity and Access Management
   a) Authentication Methods
   b) Role-Based Access Control
10. Disaster Planning and Recovery
    a) Disaster Planning
    b) Disaster Recovery Plan
11. The Economics and Ethics of Cybersecurity
    a) Economics of Security
    b) Ethical Considerations

D. OUTLINE OF MAJOR CONTENT AREAS: Continued. . .

12. Assessing Enterprise Security Posture
    a) What is Security Posture?
    b) Improving Security Posture

E. LEARNING OUTCOMES (GENERAL): The student will be able to:

1. Design security architecture focusing on security and compliance.
2. Classify attack vectors and assess device vulnerabilities.
3. Define and implement secure architecture and design through defense in depth.
4. Analyze threat detections and assess proper incident response procedures.
5. Define and implement identity and access management, including end-to-end security.
6. Develop risk assessments and implement risk-aware security controls.
7. Discern the differences between regulatory and compliance standards and how to apply standards.

F. LEARNING OUTCOMES (MNTC): NA

G. METHODS FOR EVALUATION OF STUDENT LEARNING: Methods may include but are not limited to:

1. Tests
2. Lab Exercises
3. Programming assignments
4. Comprehensive Final Exam

H. RCTC CORE OUTCOME(S). This course contributes to meeting the following RCTC Core Outcome(s):
Critical Thinking. Students will think systematically and explore information thoroughly before accepting or formulating a position or conclusion.

I. **SPECIAL INFORMATION (if any):** None