ROCHESTER COMMUNITY AND TECHNICAL COLLEGE

COMMON COURSE OUTLINE

Course discipline/number/title: COMP 2503: Cybersecurity Capstone

A. CATALOG DESCRIPTION

1. **Credits: 3**
2. **Hours/Week: 3**
3. **Prerequisites (Course discipline/number):** COMP 2048,
4. **Other requirements:** This class should be taken in the final semester of the cybersecurity program.
5. **MnTC Goals (if any):** NA

B. COURSE DESCRIPTION: This course serves as the culmination of the Cybersecurity AAS degree program. Students will demonstrate their technical and professional capabilities through a comprehensive capstone project focusing on real-world cybersecurity challenges. Students will apply security principles, tools, and methodologies learned throughout their program while developing essential professional skills for the cybersecurity industry. The course combines guided professional development with independent technical work, allowing students to showcase their ability to analyze, implement, and communicate security solutions. It is expected that this class will be taken concurrently with or after completing COMP 2049.

C. DATE LAST REVISED (Month, year): December, 2024

D. OUTLINE OF MAJOR CONTENT AREAS:

1. Security and Risk Management
   a) Risk assessment
   b) Security governance principles
   c) Compliance requirements
   d) Business continuity planning
2. Technical Security Implementation
   a) Asset security
   b) Security architecture and engineering
   c) Identity and access management
   d) Network security controls
   e) Security operations
   f) Secure software development concepts
3. Security Assessment and Testing
   a) Vulnerability assessment
   b) Penetration testing methodology
4. Documentation and Reporting
   a) Technical documentation
   b) Security policies and procedures
   c) Incident reports
   d) Executive summaries
5. Professional Development for Cybersecurity Careers
   a) Resume writing for security roles
   b) Technical interview preparation
   c) Security certifications overview
   d) Professional networking in cybersecurity
   e) Ethics in cybersecurity

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

1. Develop comprehensive security solutions aligned with risk management principles.
2. Implement asset security controls and data classification schemes.
3. Apply security architecture principles in system design.
4. Design and implement network security controls.
5. Develop identity and access management solutions.
6. Conduct security assessments and testing.
7. Implement security operations procedures and incident response.
8. Apply secure development principles in software projects.

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

9. Create professional security documentation and reports.
10. Present technical findings to both technical and non-technical audiences.
11. Develop a professional portfolio showcasing security projects and skills.
12. Demonstrate interview skills specific to cybersecurity positions.
13. Apply ethical considerations in security decision-making.

F. LEARNING OUTCOMES (MNTC): NA

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

1. Capstone Project
   a) Technical implementation
   b) Documentation
   c) Presentation
2. Professional Development Portfolio
   a) Resume and cover letter
   b) Mock interview performance

H. RCTC CORE OUTCOME(S). This course contributes to meeting the following RCTC Core Outcome(s):
Personal and Professional Accountability. Students will take responsibility as active learners for achieving their educational and personal goals.

I. SPECIAL INFORMATION (if any): None