RCTC PROGRAM PLAN

CYBERSECURITY

Associate of Applied Science

I. MINNESOTA TRANSFER CURRICULUM (MnTC)/ GENERAL EDUCATION REQUIREMENTS.....19 CREDITS

GOAL 1: WRITTEN AND ORAL COMMUNICATION .....7 CR

ENGL 1117, Reading and Writing Critically I, 4 cr
COMM 1114: Fundamentals of Public Speaking, 3 cr **OR**
COMM 1130: Interpersonal Communication, 3 cr

GOAL 4: MATHEMATICS AND LOGICAL REASONING.....3 CR

MATH 1115, College Algebra, 3 cr **OR**
MATH 1119, Applied Calculus, 3 cr **OR**
MATH 1127, Calculus I, 5 cr **OR**
MATH 2208: Fundamentals of Statistics, 4 cr

Students who intend to pursue a BS after completing their AAS should consult with their advisor as to an appropriate choice. This may involve taking additional mathematics beyond the classes listed here.

GOAL 5: HISTORY AND THE SOCIAL AND BEHAVIORAL SCIENCES.....6 CR

Recommended Courses:
ECON 1101, Introduction to Economics, 3 cr **OR**
ECON 2214, Microeconomics, 4 cr
POLS 1615, Introduction to American Government, 3 cr

GOAL 6: HUMANITIES AND THE FINE ARTS.....3 CR

Recommended Course:
PHIL 1050, Computing and AI Ethics, 3 cr

II. PROGRAM CORE REQUIREMENTS.....30 CREDITS

COMP 1140, Intro to Database & SQL, 3 cr
COMP 1150, Computer Science Concepts, 3 cr
COMP 1010, Linux Operating Systems, 3 cr
COMP 1080, Networking Protocols and Analysis, 4 cr
COMP 2243, Programming & Problem Solving, 4 cr
COMP 2275, Computer Architecture, 4 cr
COMP 2048, Introduction to Cybersecurity, 4 cr
COMP 2049, Cybersecurity Systems, 4 cr
COMP 2502, Cybersecurity Internship, 1-3 cr **OR**
COMP 2503, Cybersecurity Capstone

III. PROGRAM ELECTIVE COURSES.....11 CREDITS

RCTC PROGRAM PLAN

Any classes numbered 1000 or above to achieve a total of 60 credits.

TOTAL ..... 60 CREDITS

PROGRAM OUTCOMES:

Upon completing of the Cybersecurity Program at RCTC, students will:

1. Acquire a comprehensive understanding of cybersecurity principles and practices, including threat identification, risk management, and incident response.
2. Become proficient in programming languages such as Python, enabling them to develop secure software solutions and automate tasks.
3. Use their knowledge of computer architecture to identify and mediate vulnerabilities.
4. Gain expertise in SQL, allowing them to manage databases securely and understand the vulnerabilities associated with database systems.
5. Secure network communications and identify vulnerabilities within a network.
6. Develop a nuanced understanding of the legal and ethical considerations in cybersecurity.
7. Gain hands-on experience in real-world cybersecurity scenarios, enhancing their readiness for the job market.

This program will prepare students to take the CompTIA Security+ and CompTIA CySa+ exams. The program aligns to the standards set forth by the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program.

Revised: 2/11/2025
Implementation: Fall 2025