MASTER COURSE OUTLINE

A. CPRO 2131 Artificial Intelligence for Cybersecurity

B. COURSE DESCRIPTION:

In this course, students will explore the intersection of artificial intelligence (AI) and Cybersecurity, gaining a comprehensive understanding of how AI technologies can be leveraged to enhance cyber defense mechanisms. The curriculum covers various topics, including machine learning algorithms, anomaly detection, threat intelligence, and automated response systems. Through hands-on projects and real-world case studies, students will learn to design, implement, and evaluate AI-driven solutions to combat cyber threats. By the end of the course, participants will be equipped with the skills and knowledge to apply AI techniques in safeguarding digital infrastructures and mitigating cyber risks. Prerequisites: CPRO 2000 Network Security Fundamentals or instructor approval for individuals pursuing professional development.
(3 Cr – 3 lect, 0 lab)

C. *Core Theme: Critical Thinking

D. RIVERLAND INSTITUTIONAL LEARNING OUTCOMES:

This course addresses the following Riverland Institutional Learning Outcome(s):
☒ ILO 1: critical thinking *(Core Theme Goal 2)*
☐ ILO 2: awareness of the larger global community *(Core Theme Goal 7 or 8)*
☐ ILO 3: ethical, engaged citizenship *(Core Theme Goal 9 or Goal 10)*
☐ ILO 4: communication and collaboration *(Discipline Goal 1 and by any learning outcome(s) involving communication or collaboration)*

E. MAJOR CONTENT AREAS:

At the completion of this course, students will have knowledge and skills in:

- Artificial Intelligence Cybersecurity History
- Artificial Intelligence Cybersecurity Concepts
- Artificial Intelligence Machine Learning Models
- Artificial Intelligence Cybersecurity Algorithms
- Artificial Intelligence Cybersecurity Methods
- Artificial Intelligence Cybersecurity Applications
- Artificial Intelligence Cybersecurity Predictive Analysis
- Artificial Intelligence Cybersecurity Threat Detection
- Artificial Intelligence Cybersecurity Threat Management

- Artificial Intelligence Cybersecurity Response
- Artificial Intelligence Cybersecurity Administration

F. GOAL TYPES, OBJECTIVES, AND OUTCOMES:

GOAL	**OBJECTIVES** **Students will be able to**	**OUTCOMES** **The student will successfully**
*Critical Thinking	imagine and seek out a variety of possible goals, assumptions, interpretations, or perspectives which can give alternative meanings or solutions to given situations or problems.	1. identify and understand the different machine learning models, algorithms, tools and methods, and AI algorithms used in artificial intelligence for Cybersecurity; then use this knowledge to monitor, analyze, and respond to security events, thus protecting systems from Cybersecurity risks, threats, and vulnerabilities.
CS	demonstrate knowledge and expertise in the fundamental principles of Artificial Intelligence for Cybersecurity.	1. explain key AI concepts and how they apply to Cybersecurity.
CS	demonstrate the ability to analyze cybersecurity scenarios and proposed AI-based solutions.	1. describe various Cybersecurity threat scenarios using the appropriate AI-based solution that best addresses a particular threat.
CS	demonstrate knowledge and expertise in the AI models used to detect and respond to cyber threats.	1. develop and deploy AI models to detect and respond to Cybersecurity threats.
CS	demonstrate knowledge and expertise in using AI for Cybersecurity incident response.	1. describe AI Cybersecurity and technologies used to detect and identify Cybersecurity compromises, then implement methods to eliminate and mitigate security issues.
CS	demonstrate knowledge and expertise in using AI for Cybersecurity post-exploitation assessment.	1. use AI to analyze attack vectors, identify compromised systems, and assess the extent of the damage.
CS	demonstrate knowledge and expertise in using AI for Cybersecurity post-exploitation remediation (SECOPS).	1. develop and implement remediation plans based on their post-exploitation assessment. This will include using AI to automate vulnerability patching, restoring affected systems, and improving defenses to prevent future incidents.
CS	demonstrate business and interpersonal skills.	1. collaborate with classmates to develop security policies and share information security techniques and strategies.

G. SPECIAL INFORMATION:

This course requires Internet access, the submission of electronically prepared documents and the use of a course management software program. Students who have a disability and need accommodations should contact Accessibility Services at the beginning of the semester.

H. COURSE CODING INFORMATION:

Course Code T/Class Maximum 30; Letter Grade

Revision date: 01/07/25
AASC Approval date: 11/19/24; 02/18/25

*These five MnTC Goals have been identified as Riverland Community College Core Themes. Every course in the Riverland Community College curriculum shall meet outcomes from one of these themes.
**These five MnTC Goals have been identified as Riverland Community College Disciplines. Riverland's MnTC courses also shall meet outcomes from a Discipline Area.

NOTE: The Minnesota Transfer Curriculum "10 Goal Areas of Emphasis" are reflected in the five required discipline areas and five core themes noted in the Riverland Community College program of study guide and/or college catalog.

***Riverland Community College Core Themes**	**MnTC Goal Number**
Critical Thinking (CT)	**2**
Human Diversity (HD)	**7A, 7B, 7A/B**
Global Perspective (GP)	**8**
Ethical and Civic Responsibility (EC)	**9**
People and the Environment (PE)	**10**

****Riverland Community College Discipline Areas**	**MnTC Goal Number**
Communication (CM)	**1**
Natural Sciences (NS)	**3**
Mathematics/Logical Reasoning (MA)	**4**
History and the Social & Behavioral Sciences (SS)	**5**
Humanities and Fine Arts (HU)	**6**