Certificate

Artificial Intelligence (AI) in Cyber Defense Certificate

The Graduate Certificate in Artificial Intelligence in Cyber Defense is designed to educate students in methods to prevent, detect, and responding to cyber threats in a timely manner. Cyber defense specifically focuses on defending against external threats and attacks. The application of Artificial Intelligence (AI) to Cyber Defense can assist in monitoring for abnormalities in data access and predicting potential threats to prevent compromise to information or infrastructure.

Admission Information

The following admission requirements will apply to all applicants. All students must:

- Submit a completed online application and the application fee.
- Submit transcripts of all undergraduate and graduate work from regionally accredited institutions.
- Have earned a baccalaureate degree from a regionally accredited institution of higher education, or international equivalent.

Applicants who have not earned a degree in the United States must also submit:

- Current scores on the Test of English as a Foreign Language (TOEFL), with a minimum score of 230 on the computer-based TOEFL or 80 on the TOEFL iBT.

Curriculum Requirements

The certificate is awarded based upon the student's successful completion of 12* credit hours of graduate level courses:

AI/CYSE 510	Artificial Intelligence (AI) Methods and Models	3
AI/PHIL 546	Artificial Intelligence (AI) Ethics and Policy	3
AI/CYSE 521	Generative AI in Cybersecurity	3
CYSE 520	Applied Machine Learning in Cybersecurity	3
AI Practicum *		0
Total Credit Hours		**12**

*	AI 669/DASC 669