|  |  |
| --- | --- |
|  | **SOUTH DAKOTA BOARD OF REGENTS**  ACADEMIC AFFAIRS FORMS |
| New Course Request |
|  |  |

| **DSU** |  | **Beacom College of Computer and Cyber Sciences** | | |
| --- | --- | --- | --- | --- |
| **Institution** |  | **Division/Department** | | |
|  | | |  |  |
| **Institutional Approval Signature** | | |  | **Date** |

|  |
| --- |

**Section 1. Course Title and Description**

| **Prefix & No.** | **Course Title** | **Credits** |
| --- | --- | --- |
| CSC 382 | Adversarial AI and Security | 3 |

| **Course Description** |  |
| --- | --- |
| This course examines AI’s role in cybersecurity, focusing on adversarial attacks, defense strategies, and AI-driven security assessments. Students will learn to manipulate and defend AI models, assess vulnerabilities, and apply AI tools for threat mitigation. Hands-on projects and case studies develop practical skills for securing AI systems. | |

**Pre-requisites or Co-requisites**

| **Prefix & No.** | **Course Title** | **Pre-Req/Co-Req?** |
| --- | --- | --- |
| CSC 134 | Intro to Cyber | Pre-Req |
| CSC 247  Or  CSC 447 | Introduction to Artificial Intelligence  Or  Artificial Intelligence | Pre-Req |

**Registration Restrictions**

|  |
| --- |
| None |

**Section 2. Review of Course**

1. **Will this be a unique or common course (*place an “X” in the appropriate box*)?**

|  |  |
| --- | --- |
|  | **Unique Course**  *If the request is for a unique course, institutions must review the common course catalog in the system course database to determine if a comparable common course already exists. List the two closest course matches in the common course catalog and provide a brief narrative explaining why the proposed course differs from those listed. If a search of the common course catalog determines an existing common course exists, complete the Authority to Offer an Existing Course Form. Courses requested without an attempt to find comparable courses will not be reviewed.* |

|  |  |  |
| --- | --- | --- |
| **Prefix & No.** | **Course Title** | **Credits** |
| CSC 723 | Machine Learning for Cyber Security | 3 |
| *Provide explanation of differences between proposed course and existing system catalog courses below:* | | |
| The proposed course has a focus specifically on how AI/ML systems can be attacked and defended, exploring adversarial machine learning, attacker/defender objectives, robustness testing, and security implications of deploying AI models. Whereas this graduate course Applies ML as a tool to solve traditional cybersecurity problems, such as intrusion detection, anomaly detection, and profiling. The emphasis is on using ML to improve cyber defenses, not on how ML itself can be a security target. | | |

**Section 3. Other Course Information**

**3.1. Are there instructional staffing impacts?**

☒ No. Schedule Management, explain below: The course will be offered on a rotating year and semester schedule. It is not anticipated that additional faculty will be needed to deliver this course.

**3.2. Existing program(s) in which course will be offered:** BSAI, AI Cyber (New Minor)

**3.3. Proposed instructional method by university *(as defined by*** [*AAC Guideline 5.4*](https://www.sdbor.edu/administrative-offices/academics/academic-affairs-guidelines/Documents/5_Guidelines/5_4_Guideline.pdf)***)*:** R - Lecture

**3.4. Proposed delivery method by university *(as defined by*** [*AAC Guideline 5.5*](https://www.sdbor.edu/administrative-offices/academics/academic-affairs-guidelines/Documents/5_Guidelines/5_5_Guideline.pdf)***)*:** 001 - Face to Face, 015 - Online Asynchronous

**3.5. Term change will be effective:** Fall 2025

**3.6. Can students repeat the course for additional credit?** ☐Yes, total credit limit: ☒ No

**3.7. Will grade for this course be limited to S/U (pass/fail)?** ☐Yes☒No

**3.8. Will section enrollment be capped?** ☒Yes, max per section: 25 ☐ No

**3.9. Will this course equate (i.e., be considered the same course for degree completion) with any other unique or common courses in the common course system database in Colleague and the Course Inventory Report?** ☐Yes ☒ No

**3.10. Is this prefix approved for your university?** ☒ Yes ☐ No

**Section 4. Department and Course Codes (Completed by University Academic Affairs)**

|  |  |
| --- | --- |
| 1. **University Department:** | Computer Science |

|  |  |
| --- | --- |
| 1. **Banner Department Code:** | DSCI |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. **Proposed** [**CIP Code**](http://nces.ed.gov/ipeds/cipcode/default.aspx?y=55)**:** | 11.0102 | | | | |
|  |  | | | | |
| *Is this a new CIP code for the university?* | |  | Yes |  | No |