New Certificate: Cybersecurity

CALIFORNIA STATE UNIVERSITY SAN MARCOS
NEW PROGRAM PROPOSAL – P Form Signature

For Academic Programs Office Use Only
R.E. Catalog File

COLLEGE ☐ CHABSS ☒ CoBA ☐ CoEHHS ☐ CSM

TITLE OF PROGRAM Cybersecurity –Management, Risk & Governance Discipline MIS

This form is the signature sheet for new programs and new options/concentrations/emphases/tracks within existing programs. For all changes to existing programs (other than addition of new options/concentrations/emphases/tracks), use the Form P-2.

Check one:
- ☐ New Undergraduate Major or New Graduate Degree — Attach a completed New Program Template
- ☐ New Option/Concentration/Emphasis/Track
- ☐ New Minor
- ☐ New Teaching Credential
- ☒ New Certificate

} Attach a completed New Option/Concentration/ Special Emphasis, Teaching Credential and Minor

Attach a completed New Certificate Template

Does this proposal impact other disciplines? ☐ Yes ☒ No If yes, obtain signature(s).
Any objections or concerns should be stated in writing and attached to this form. Please check the box to indicate whether a memo has been attached.

Term and Academic Year of intended implementation (e.g. Fall 2016): Fall 2018

Discipline #1	_____Support _____Oppose	
Signature	☐ Date	Youwen Ouyang
Discipline #2	_____Support _____Oppose	
Signature	☐ Date	
Discipline #3	_____Support _____Oppose	
Signature	☐ Date	
Discipline #4	_____Support _____Oppose	
Signature	☐ Date	
Discipline #5	_____Support _____Oppose	
Signature	☐ Date	

RECEIVED
APR 20 2018
BY:

CALIFORNIA STATE UNIVERSITY
SAN MARCOS

Procedure for Submitting Proposals for New Certificates

1. Full and exact title of the Certificate program and level of the program (Certificate of Specialized vs. Advanced Study). Name and position of the person(s) submitting the proposed Certificate. Intended implementation date of the program.

Title: Cybersecurity – Management, Risk & Governance
Level: Advanced Study
Name: Teresa Macklin
Position: Program Director, Cybersecurity PSM (Interim)
Implementation date: Fall, 2018

2. List of the existing programs in the discipline(s) under which the new Certificate is to be offered.

This program will be offered by MIS through Extended Learning, in partnership with the Cybersecurity Professional Science Masters.

3. List of the existing program(s) that may be affected by the proposed Certificate.

It may affect the Cybersecurity Professional Science Masters, but this certificate is proposed and managed by the same committee.

4. Purpose of the proposed Certificate, including specific academic objectives served, professional applications, potential student market, and a statement explaining the need for the Certificate in comparison to existing related majors, minors, and Graduate programs.

Purpose: There is a broad need for these skills. Demand for the information and skills provided by this certificate remains very high, yet many potential students are not prepared to embark on a full Master's program. Additionally, some career paths do not require a master's degree. Many organizations will support funding employee certification over a Master's program. Further, many potential students do not require, or are not prepared for the technical aspects of cybersecurity.

Academic Objectives: This certificate is intended to provide students with knowledge, skills and experience sufficient for them to develop and/or manage the implement of a cybersecurity program in an organization which stores or transmits protected information. Please note that a complementary certificate, "Cybersecurity – Technologies", which explores the security of computer and network technologies.

Compared to existing programs: The MIS program has a 2 unit elective, "MIS 418 Information Security Management" that cover some of the matrial in the MCS500 course. At present there are no programs on campus teaching the remaining topics. The Cybersecurity Master's program includes these courses.

5. List of the courses, by catalog number, title, and units of credit, as well as total units to be required under the proposed Certificate.

MCS 500	***Introduction to Cybersecurity (2)***
MGMT 521	***Principles of Organizational Behavior and Leadership for Security Management (2)***
MIS 522	***Information Systems and Security Management (2)***
MIS 621	***Information Security Governance (3)***
MIS 622	***Technology Assessment and Security Risk Management (3)***

6. Definition of the minimum level of competence to be demonstrated to earn the proposed Certificate, and a description of the means of assessing that competence (examination, practicum, field experience, etc.).

These courses require a combination of written and oral communication skills demonstrated by a series of papers and presentations. These, along with quizzes and other assessments are used to assign grades. Students must maintain a 3.0 GPA and earn at least a "C" (2.0) in each course.

7. Description of assessment strategies for waiver of lower division requirements (where applicable).

N/A

8. New courses to be developed. Include proposed catalog descriptions in the Certificate proposal. "C-forms" for these courses should accompany the proposed Certificate package for curricular review.

N/A

9. List of all present faculty members, with rank, appointment status, highest degree earned, date and field of highest degree, and professional experience, who would teach in the proposed aggregate of courses.

Dr Yi Sun, Professor,
Full Time TTF, PhD Decision and Information Sciences, 2003

Dr Jeff Kohles, Professor,
Full Time TTF, PhD Leadership and Organizational Behavior

Teresa Macklin, Lecturer/Associate Dean IITS,
Full Time Administrator, JD Law, 2007

10. Instructional resources (faculty, space, equipment, library volumes, etc.) needed to implement and sustain the Certificate program.

This certificate program will use open seats in the existing Cybersecurity Professional Science Master's program. At present we do not anticipate creating new sections of these programs to meet demand for the certificate.

P-FORM PREPARATION

1a. Yi Sun — 02.06.2017
Originator (Please print) — Date

1b. _____ — 1/4/18
Librarian Liaison for Library Report+ — Date

1c. _____ — 1/16/18
IITS Liaison for IITS Report+ — Date

PROGRAM/DEPARTMENT-LEVEL REVIEW

2. _____ — 12/14/17
Program/Department - Director/Chair* — Date

COLLEGE/SCHOOL-LEVEL REVIEW

3. _____ — 1/12/17
College/School Curriculum Committee* — Date

REVIEW (Signatures must be obtained by proposer)

4a. _____ — 2/3/18
Vice President for Student Affairs* — Date

4b. _____ — 1/8/18
Dean of Library* — Date

4c. _____ — 1/16/18
Dean of Information and Instructional Technology Services* — Date

4d. _____ — 1/18/2018
Vice President for Finance and Administrative Services* — Date

4e. _____ — 2/14/18
Dean of Graduate Studies (if applicable) * — Date

COLLEGE/SCHOOL-LEVEL RECOMMENDATION

5. _____ — 12/15/17
College/School Dean/Director* — Date

UNIVERSITY-LEVEL REVIEW
(May not begin until all signatures numbered 1-5 have been obtained.)

6a. _____ — _____
University Curriculum Committee^ — Date

6b. _____ — _____
Budget and Long-Range Planning Committee^ — Date

FACULTY APPROVAL

7. _____ — _____
Academic Senate — Date

UNIVERSITY-LEVEL APPROVAL

8. _____ — _____
Provost — Date

9. _____
Date to Chancellor's Office

+ Please contact the liaisons at the beginning of the process and allow sufficient time for the liaisons to prepare the resource implication report. Upon completion of the report liaisons will sign.
* May attach a memo on program impact on the unit and the ability of the unit to support it.
^ Attach a memo summarizing the curricular and/or resource deliberations.
o summarizing the curricular and/or resource deliberations.