CALIFORNIA STATE UNIVERSITY SAN MARCOS

For Academic Programs Office Use Only
R. E. _____ Catalog_____File____

PROGRAM CHANGE PROPOSAL - Form P-2

COLLEGE ☐ CHABSS ☐ CoBA ☐ CoEHHS ☒ CSM

TITLE OF PROGRAM Master of Cybersecurity Discipline

Check one: ☒ Change to Program ☐ Program Deletion

TITLE OF DEGREE PROGRAM: Master of Cybersecurity

This form is the signature sheet for a change to, or deletion of, an existing program.
Note that the addition of a new option/concentration/emphasis/track is a new "program," and requires the use of Form P.

For a change to a program,

1. Attach a page (or pages) giving a brief summary of the purpose of this proposal, and its connection to the mission and student learning outcomes of the program.
2. Attach catalog copy showing exactly how the program should appear in the catalog if the changes are approved.

For a program deletion, attach a statement explaining the impact on students: how will the program be "taught-out" for declared majors?

Does this proposal impact other disciplines or units? _____Yes __X__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.

____ Discipline/Unit	_____ Signature	☐	_____ Date	_____Support _____Oppose
____ Discipline/Unit	_____ Signature	☐	_____ Date	_____Support _____Oppose
____ Discipline/Unit	_____ Signature	☐	_____ Date	_____Support _____Oppose
____ Discipline/Unit	_____ Signature	☐	_____ Date	_____Support _____Oppose

1. Rika Yoshii 3-23-16
Originator (Please Print) Date

Program/ Department - Director/Chair 5-3-16 Date

APPROVAL PROCESS

3. _____ ☐ 5/2/2016
College Curriculum Committee^ Date

4. _____ ☐ 5/3/16
College Dean (or Designee)* Date

5a. _____ ☐ _____
University Curriculum Committee^ Date

5b. _____ ☐ _____
Budget and Long-Range Planning Committee (if applicable)^ Date

6. _____ _____
Academic Senate Date

7. _____ _____
Provost (or Designee) Date

8. _____ _____
President Date

9. _____
Date to Chancellor's Office (if applicable)

* Where appropriate, attach a memo on program impact on the unit and the ability of the unit to support it. Check the box next to the signature line to indicate whether a memo has been attached.
^ Where appropriate, attach a memo summarizing the curricular and/or resource deliberations. Check the box next to the signature line to indicate whether a memo has been attached.

RECEIVED
MAY 03 2016
BY:_____

Changes to the Master in Cybersecurity Catalog Description.

MCS 500 Introduction to Cybersecurity being proposed (C-form) will replace MCS660 as a required course. While MCS660 (a generic communication class) may be useful, the communication aspect is covered in the MIS and MBA courses in context since this is a Professional Science Master's program. On the other hand, we never had an Introduction course and this lack has caused problems for the current cohort. Based on this experience, we are proposing MCS500 as a required introduction course. The number of required unit will remain the same

MCS 597 being proposed (C-form) in addition to MCS 697 is now available in lieu of a required course.

Please see the attached catalog description with the changes in red.

Cover Letter

To the Curriculum Review Committees

The Steering Committee of Masers in Cybersecurity recently went through an extensive review of all courses and decided to make two corrections: MCS510 description change and MCS611 name change. The corrections better reflect the true content of the courses. MCS611 will be taught in Fall 2016 while MCS510 will be taught in Spring 2017. (two C2-forms).

The course outlines do not change, but I am resubmitting them.

The second change is to replace MCS660 with MCS500 for the set of required courses.

While MCS660 (a generic communication class) may be useful, the communication aspect is covered in the MIS and MBA courses in context since this is a Professional Science Master's program. On the other hand, we never had an Introduction course and this lack has caused problems for the current cohort. Based on this experience, we are proposing MCS500 as a required introduction course. The number of required unit will remain the same (C-form and P2-form).

Finally, we are proposing MCS597 Special Topics. Many professional students enter the program with prior knowledge equivalent of our required courses. In such cases, instead of offering independent directed study to many students, we would like to offer a special topics course in lieu of the required course. (C-form)

If you have any questions, please contact ryoshii@csusm.edu. I am the interim program director.

Thank you very much.

Rika Yoshii

3-23-2016

CYBERSECURITY*

Programs

The Master of Science in Cybersecurity is a professional science degree program designed to meet the needs of the computing industry and associated organizations. The program is a blend of technical courses and business courses with a capstone project. The objective of the program is to train an expertly skilled workforce to fulfill the imminent needs of the emerging and evolving cybersecurity industry. The program is designed to prepare those with strong background in computer science for management positions in cybersecurity such as the manager of the information security department, the director of risk assessment and compliance, the chief information security officer, the director of IT security, and project managers of security related projects.

Throughout the program, students will be exposed to real-world problems/cases, leading-edge technologies, managerial/interpersonal skills, ethics and governance knowledge, and problem solving skills.

The rigorous program is taught in the evenings and on weekends to accommodate the working student. The program design is a cohort model that requires students to go through the program together over a five-semester period with a predetermined course sequence. It is a non-thesis degree program requiring a rigorous "Internship or Semester-In-Residence" project as culminating experience.

Each student will be guided and evaluated by an Advisory Committee that will be made up of university faculty, program instructors, and industry mentors, as well as program advisors.

Admission Requirements and Application

- Admission decisions will be made by the Admission Committee chosen by the Program Director in consultation with its faculty
- Admission decisions will be based on 1) undergraduate courses and GPA, 2) GRE scores, 3) TOEFL for some students **, and 4) the statement of purpose and recommendation letters.
- Admission to the program requires an undergraduate degree in computer science or closely related discipline, and should include upper-division courses in operating systems, networks and software engineering. Applicants with a baccalaureate degree in a related field may be able to meet pre-requisites with equivalent work experiences in computer science and will be considered for conditional admission.
- Admission requires a minimum of 3.0 grade point average in the upper-division computer science courses and at least a 2.5 undergraduate GPA in the last 60 semester units (or last 90 quarter units) attempted.

**The M.S. in Cybersecurity is offered through the Office of Extended Learning.*

***All applicants must have a TOEFL score of 80 iBT or above (213 on the computer-based examination, 550 paper-based), or an IELTS score of 6.0, unless they possess a bachelor's degree from a post-secondary institution where English was the principal language of instruction.*

- All applicants must submit general GRE scores when applying. Minimum GRE scores required are:
  - Verbal 143
  - Quantitative 155
  - Analytical Writing 3.5 (this will also satisfy the Graduate Writing Assessment Requirement)

Applicants must submit:

1. The program application form.
2. The statement of purpose outlining the reason or pursuing the degree.
3. GRE scores.
4. TOEFL score if required.
5. One set of transcripts from all colleges/universities attended.
6. Two recommendation letters on a provided form.

- Applicants to the program will be subject to standard background checks in accordance with Defense Security Service reporting requirements.

Student candidates may apply at any time throughout the year. However, selection and admission will be completed by early May for the fall semester start. Later applications will be considered, as spaces remain available. Feedback to applicants, but not final admission decisions, will be provided on a timely basis regardless of the time of application.

Degree Requirements and Courses

The Master of Cybersecurity requires thirty-eight (38) semester hours of coursework. Students must complete a set of courses and the culminating experience project with a 3.0 GPA and earn at least a "C" (2.0) in each course.

Seven Required Technical Side Courses (23 units)	
MCS 510	3
MCS 511	3
MCS 512	4
MATH 503	3
MCS 610	4
MCS 611	4
MCS 500	2

Four Required Business Side Courses (10 units)	
MGMT 521	2
MIS 522	2
MIS 621	3
MIS 622	3

Culminating Experience Total (5 units)	
MCS 680A	1
MCS 680B	4
Total Units	***38***

A student who has obtained a waiver for a required course may enroll in MCS597 Topics in Cybersecurity or MCS 697 Directed Studies upon consent of the instructor.

Continuation

Graduate students must maintain an overall GPA of 3.0 and earn at least a C (2.0) in each course, except those taken for credit/no credit. Any student whose overall GPA falls below 3.0 for two consecutive semesters will be dropped from the program. A full-time student should be enrolled in the predetermined course schedule and credit hours each semester for the program.

Advancement to Candidacy

The student will advance to Master's Degree candidacy upon the completion of MCS680A and approval of a Project Abstract by the student's Advisory Committee. The Advisory Committee is made up of a program faculty member, an industry mentor, and the Program Director.

Culminating Experience

All students must enroll in MCS 680A/B Internship/Semester in Residence and successfully complete a 16-week project in lieu of a research thesis. Completion and defense of the culminating experience project results in an oral defense and a substantial technically written report. Student projects will address and affect real-world challenges in cybersecurity. Students will demonstrate their ability to integrate principals of science and technology with fundamental business practices. The type of experience and nature of the project will vary, depending upon the student's background, employment, and right-to-work status. A substantive written project report must be submitted, orally defended, and approved at the end of the Internship/Semester-In-Residence. In unusual circumstances where project requirements are not completed, defended, and approved at the end of MCS 680B, a student may complete the requirements within six months under the guidance of the advisory committee. In such cases, enrollment in MCS 699 is required.