

CERTIFICATE IN CYBERSECURITY FOUNDATIONS



SACRAMENTO STATE

In Workflow

1. CBA College Committee Chair (ramakrishna.dantu@csus.edu)
2. CBA Dean (ptong@csus.edu)
3. Academic Services (catalog@csus.edu)
4. Senate Curriculum Subcommittee Chair (curriculum@csus.edu)
5. Faculty Senate Executive Committee Chair (kathy.honeychurch@csus.edu)
6. Faculty Senate Chair (kathy.honeychurch@csus.edu)
7. Dean of Graduate (s.storms@csus.edu)
8. Dean of Undergraduate (shaw@csus.edu)
9. Provost (maguirem@csus.edu)
10. President (khtudor@csus.edu)
11. Chancellor's Office (s.storms@csus.edu)
12. Board of Trustees (torsetj@csus.edu)
13. WASC (elisa.trimboli@csus.edu)
14. Catalog Editor (catalog@csus.edu)
15. Graduate Studies (jdsmall@csus.edu; mxiong@csus.edu)
16. Registrar's Office (k.mcfarland@csus.edu)

Approval Path

1. Fri, 23 May 2025 20:18:24 GMT
Katie Dickson (katiedickson): Rollback to Initiator
2. 2026-06-02T19:24:33Z
Tota Panggabean (panggabean): Rollback to Initiator
3. 2026-09-25T19:28:17Z
Ramakrishna Dantu (ramakrishna.dantu): Approved for CBA College Committee Chair
4. 2026-09-25T20:18:56Z
Pingsheng Tong (ptong): Approved for CBA Dean

New Program Proposal

Date Submitted: 2026-09-10T18:48:31Z

Viewing: Certificate in Cybersecurity Foundations

Last edit: 2026-09-10T18:48:29Z

Changes proposed by: Zahra Aivazpour (223025621)

Academic Group: (College)

Business

Academic Organization: (Department)

Information Systems and Business Analytics

Catalog Year Effective:

2027-2028 Catalog

NOTE: This degree major program will be subject to program review evaluation within six years after implementation.

Individual(s) primarily responsible for drafting the proposed degree major program:

Name (First Last)	Email	Phone 999-999-9999
Zahra Aivazpour	zahra.aivazpour@csus.edu	916-278-7123

Program Snapshot**Type of Program:**

Certificate

Title of the Program:

Certificate in Cybersecurity Foundations

Designation: (degree terminology)

Certificate - Graduate

Delivery Mode:

Fully Face to Face

Hybrid

Fully Online

Support Mode:

Self Support

What is the instructional modality of all courses in this program?

Asynchronous

Synchronous

Both Asynchronous and Synchronous

Please see the CSU/CIP Code Crosswalk: https://www.calstate.edu/csu-system/administration/academic-affairs/academic-programs-innovation-and-faculty-development/Documents/CSU_Codes_to_CIP_2020.pdf

Is this a pilot program?

No

Establishment of a master's degree program should be preceded by a national professional accreditation of the corresponding bachelor's degree major program.

Will this program require accreditation?

No

Provide a clear, concise overview of the program proposal (new or change) and provide a justification. For NEW programs describe the purpose and focus of the program, identify the target student population(s), and highlight key strengths and distinguishing features of the program.

The Certificate in Cybersecurity Foundations is an introductory program designed to provide participants with essential knowledge and skills in cybersecurity. Covering key topics such as network security, risk management, incident response, and cryptography, the program equips individuals with the foundational tools to identify and mitigate cybersecurity threats. This certificate is ideal for IT professionals, business leaders, and anyone interested in entering the cybersecurity field, preparing them for entry-level roles and further education in cybersecurity.

Justification:

Growing Cyber Threat Landscape: With the rise in cyberattacks and data breaches, there is an urgent need for professionals who understand fundamental cybersecurity principles. This program addresses that demand by providing essential training.

Foundation for Career Advancement: As organizations prioritize cybersecurity, individuals with foundational knowledge will be better positioned for entry-level roles and further educational opportunities, making this certificate a stepping stone for career growth.

Accessibility: This program is designed for individuals from diverse backgrounds, including those with little prior experience in IT or cybersecurity, making it accessible to a wider audience.

Introduction to Certifications: This program introduces participants to courses that can help them pursue industry-recognized certifications in the future, enhancing their qualifications and employability in the cybersecurity field.

University Learning Goals

Graduate (Masters) Learning Goals:

Disciplinary knowledge
Communication
Critical thinking/analysis
Information literacy
Professionalism
Intercultural/Global perspectives

Will this program be required as part of a teaching credential program, a single subject, or multiple subject waiver program (e.g., Liberal Studies, Biology) or other school personnel preparation program (e.g., School of Nursing)?

No

Curriculum Alignment and Assessment

Program Goals

Provide a brief statement of the program's overarching goals and priorities: • Describe the program's mission, focus, and intended impact on students. • Identify broad areas of emphasis (e.g., career preparation, research, community engagement, leadership development). • Goals may be aspirational or developmental and do not need to be directly measurable.

Program Goals Statement

The Certificate in Cybersecurity Foundations aims to prepare students and working professionals with essential knowledge and skills to understand, identify, and address cybersecurity threats and risks. The program emphasizes career preparation by developing foundational knowledge in areas such as network security, risk management, incident response, and cryptography. It seeks to provide an accessible pathway into the cybersecurity field for students from diverse academic and professional backgrounds while preparing students for entry-level cybersecurity roles and further education. The program also introduces students to knowledge areas associated with industry-recognized cybersecurity certifications. Through an applied and industry-relevant curriculum, the program aims to strengthen students' cybersecurity competencies and prepare them to respond to evolving security challenges in organizations.

Program Learning Outcomes

Provide measurable, program-specific learning outcomes that reflect the most important competencies students will demonstrate upon completion of the program. Programs are expected to assess and use PLOs for continuous improvement.

Program Learning Outcomes

Learning Outcome

Develop cybersecurity and information assurance strategies to current, practical, and important contexts and situations within the field.

Communicate in writing with clarity and purpose, both within the discipline of cybersecurity and in broader contexts.

Demonstrate ability to obtain, assess, and analyze information from diverse sources in the development of cybersecurity and information assurance policies and procedures.

Articulate an understanding of professional integrity and the ethical and legal implications of the implementation of cybersecurity and information assurance.

Learning Outcomes Display

Course Code	PLO 1	PLO 2	PLO 3	PLO 4
-------------	-------	-------	-------	-------

Please attach a Comprehensive Program Assessment Plan

Assessment_Certificate_Foundations.docx

Please attach a Curriculum Map Matrix

Cybersecurity_Foundations_Certificate_Smart Planner 2025.docx

Please attach a Five-Year Budget Projection. For NEW programs, also attach a Budget Narrative.

budget_draft_foundations_certificate.xlsx

Please attach the updated roadmap:

Cybersecurity_Foundations_Certificate_Roadmap_2025.xlsx

Catalog Description (catalog copy):

The Certificate in Cybersecurity Foundations is designed to provide participants with a comprehensive introduction to the essential concepts, principles, and practices of cybersecurity. This program covers critical topics such as network security, risk management, incident response, cryptography, and security governance, equipping individuals with the foundational knowledge necessary to understand and address common cybersecurity threats and vulnerabilities.

Admission and Continuation Requirements (catalog copy): minimum GPA and prerequisites (if applicable), required coursework or preparation, portfolio, test scores, and/or letters of recommendation. For graduate programs: expectations for a relevant bachelor's degree (required or preferred disciplines, prerequisite knowledge, or equivalent experience), include evidence that program requirements conform to the minimum requirements for the culminating experience, as specified in Title 5 Section 40510 The Master's Degree and Section 40511 The Doctoral Degree.

Admission to this certificate is open to domestic and international students who meet the following criteria:

1. Academic Standing, Degree, and GPA
Four-year bachelor's degree or equivalent with a minimum GPA of 2.5

2. Statement of Purpose
Applicants must submit a Statement of Purpose describing their academic background, and professional experience.

3. Résumé
Applicants must submit a current résumé outlining relevant academic preparation, professional experience, and technical skills.

4. Letters of Recommendation
Applicants must submit two letters of recommendation from individuals who can speak to the applicant's academic ability, professional readiness, or potential for success.

5. English Language Proficiency (if applicable)
A foreign language test is required for applicants who earned their undergraduate degree from a country where the official language of instruction is not English. Applicants must submit official English proficiency scores (Institution Code: 4671) from one of the following exams taken within the past two years:

TOEFL iBT (minimum score of 4 on the ETS 1–6 scale)

IELTS: minimum band score of 6.0

PTE Academic: minimum score of 50

6. At least 6 units in financial reporting/audit and telecommunication and networking courses, with minimum grades of "C" or higher, are required for applicants with less than 3 years of cybersecurity-related work experience.

Program Requirements (catalog copy):**List of courses (Total units: 12)****Cores (9 units)**

MCM 205 Cybersecurity Foundations

MCM 206 Cybersecurity & Ethics

MCM 208 Cybersecurity Policy, Compliance, and Risk Assessment

Electives (3 units)

MCM 211 Security Practices in SDLC

ACCY 212 Forensic Accounting & Fraud Examination

MCM 213 AI and ML Techniques for Cybersecurity

MCM 214 Blockchain Technology

ACCY 216 Accounting Information systems Audit and Control

MCM 217 Data Driven Cybersecurity

Reviewer Comments:

Katie Dickson (katiedickson) (Fri, 23 May 2025 20:18:24 GMT): Rollback: In preparation for the summer 2025 Curriculum Workflow software update, all course and program proposals have been moved out of Workflow. Submissions to Workflow will resume Monday, August 11, 2025. Please contact Academic Services at catalog@csus.edu with any questions.

Tota Panggabean (panggabean) (Tue, 02 Jun 2026 19:24:33 GMT): Rollback: Additional review is required as per ADAP office.

Key: 590