Information and Cybersecurity: MICS

The Master of Information and Cybersecurity (MICS) (https://cybersecurity.berkeley.edu/form/) is an online, part-time professional degree program that provides the technical skills and contextual knowledge students need to assume leadership positions in private sector technology companies as well as government and military organizations. The interdisciplinary program offers students mastery of core technical skills and fluency in the business, political, and legal context for cybersecurity, as well as managing cyber risk in the service of strategic decision making.

Students attend weekly live ("synchronous") sessions with classmates and instructors via an online platform as well as engaging with online ("asynchronous") videos and assignments on their own time.

The core MICS curriculum includes cryptography, secure programming, systems security, and the ethical, legal, and economic framework of cybersecurity. In addition, students may select from a wide variety of electives covering topics such as privacy engineering, managing cyber risk, and usability security. MICS features a project-based approach to learning and encourages the pragmatic application of a variety of different tools and methods to solve complex problems.

Graduates of the program will be able to:

- Understand the defining challenges of cybersecurity;
- Comprehend and implement cryptosystems;
- Know the main causes of software vulnerabilities and the means to avoid and defend against them;
- Apply security principles to analyze and determine the security of a system; and
- Define the technical, process, and policy capabilities an organization needs to deploy to mitigate cyber risks to acceptable levels.

The I School also offers a master's in Information and Data Science (http://guide.berkeley.edu/graduate/degree-programs/information-data-science/) (MIDS), a master's in Information Management and Systems (http://guide.berkeley.edu/graduate/degree-programs/information-management-systems/)(MIMS), and a doctoral degree (PhD) program in Information Management and Systems (http://guide.berkeley.edu/graduate/degree-programs/information-management-systems-phd/).

Unit Requirements

The Master of Information and Cybersecurity is designed to be completed in 20 months. Students will complete 27 units of course work over five terms, taking two courses (6 units) per term for four terms and a one 3-unit capstone course in their final term. MICS classes are divided into foundation courses (9 units), a systems security requirement (3 units), advanced courses (12 units), and a synthetic capstone (3 units). Students will also complete an immersion at the UC Berkeley campus.

Curriculum

Foundation Courses		
CYBER W206	Course Not Available	3
CYBER W200	Course Not Available	3
CYBER W202	Course Not Available	3
CYBER W204	Course Not Available	
Systems Security Courses		
CYBER W210	Course Not Available	
CYBER W211	Course Not Available	
Advanced Courses		
CYBER W207	Course Not Available	
CYBER W215	Course Not Available	
CYBER W220	Course Not Available	
CYBER W233	Course Not Available	
Capstone Course		
CYBER W295	Capstone	3

Immersion

As a Master of Information and Cybersecurity (MICS) student, the immersion is your opportunity to meet faculty and peers in person on the UC Berkeley campus. You will have the opportunity to gain on-the-ground perspectives from faculty and industry leaders, meet with cybersecurity professionals, and soak up more of the School of Information (I School) culture. Offered twice a year, each four- to five-day immersion will be custom-crafted to deliver additional learning, networking, and community-building opportunities.

Please refer to the cybersecurity@berkeley website (https://cybersecurity.berkeley.edu/academics/) for more information.

Minimum Requirements for Admission

The following minimum requirements apply to all graduate programs and will be verified by the Graduate Division:

1. A bachelor’s degree or recognized equivalent from an accredited institution;
2. A grade point average of B or better (3.0);
3. If the applicant has completed a basic degree from a country or political entity (e.g., Quebec) where English is not the official language, adequate proficiency in English to do graduate work, as evidenced by a TOEFL score of at least 90 on the iBT test, 570 on the paper-and-pencil test, or an IELTS Band score of at least 7 on a 9-point scale (note that individual programs may set higher levels for any of these); and
4. Sufficient undergraduate training to do graduate work in the given field.

Applicants Who Already Hold a Graduate Degree

The Graduate Council views academic degrees not as vocational training certificates, but as evidence of broad training in research methods, independent study, and articulation of learning. Therefore, applicants who already have academic graduate degrees should be able to pursue new subject matter at an advanced level without the need to enroll in a related or similar graduate program.

Programs may consider students for an additional academic master’s or professional master’s degree only if the additional degree is in a distinctly different field.

Applicants admitted to a doctoral program that requires a master’s degree to be earned at Berkeley as a prerequisite (even though the applicant already has a master’s degree from another institution in the same or a closely allied field of study) will be permitted to undertake the second master’s degree, despite the overlap in field.

The Graduate Division will admit students for a second doctoral degree only if they meet the following guidelines:

1. Applicants with doctoral degrees may be admitted for an additional doctoral degree only if that degree program is in a general area of knowledge distinctly different from the field in which they earned their original degree. For example, a physics PhD could be admitted to a doctoral degree program in music or history; however, a student with a doctoral degree in mathematics would not be permitted to add a PhD in statistics.
2. Applicants who hold the PhD degree may be admitted to a professional doctorate or professional master's degree program if there is no duplication of training involved.

Applicants may apply only to one single degree program or one concurrent degree program per admission cycle.

Required Documents for Applications

1. **Transcripts:** Applicants may upload *unofficial* transcripts with your application for the departmental initial review. *If the applicant is admitted,* then *official* transcripts of all college-level work will be required. Official transcripts must be in sealed envelopes as issued by the school(s) attended. If you have attended Berkeley, upload your unofficial transcript with your application for the departmental initial review. *If you are admitted,* an official transcript with evidence of degree conferral *will not* be required.
2. **Letters of recommendation:** Applicants may request online letters of recommendation through the online application system. Hard copies of recommendation letters must be sent directly to the program, not the Graduate Division.
3. **Evidence of English language proficiency:** All applicants who have completed a basic degree from a country or political entity in which the official language is not English are required to submit official evidence of English language proficiency. This applies to institutions from Bangladesh, Burma, Nepal, India, Pakistan, Latin America, the Middle East, the People's Republic of China, Taiwan, Japan, Korea, Southeast Asia, most European countries, and Quebec (Canada). However, applicants who, at the time of application, have already completed at least one year of full-time academic course work with grades of B or better at a US university may submit an official transcript from the US university to fulfill this requirement. The following courses will not fulfill this requirement:
    - courses in English as a Second Language,
    - courses conducted in a language other than English,
    - courses that will be completed after the application is submitted, and
    - courses of a non-academic nature.

If applicants have previously been denied admission to Berkeley on the basis of their English language proficiency, they must submit new test scores that meet the current minimum from one of the standardized tests. Official TOEFL score reports must be sent directly from Educational Test Services (ETS). The institution code for Berkeley is 4833. Official IELTS score reports must be sent electronically from the testing center to University of California, Berkeley, Graduate Division, Sproul Hall, Rm 318 MC 5900, Berkeley, CA 94720. TOEFL and IELTS score reports are only valid for two years.

Where to Apply

Visit the Berkeley Graduate Division application page (http://grad.berkeley.edu/admissions/apply/).

Expand all course descriptions [+]Collapse all course descriptions [-]

CYBER 200 Beyond the Code: Cybersecurity in Context 3 Units

Terms offered: Not yet offered

This course explores the most important elements beyond technology that shape the playing field on which cybersecurity problems emerge and are managed. The course emphasizes how ethical, legal, and economic frameworks enable and constrain security technologies and policies. It introduces some of the most important macro-elements (such as national security considerations and interests of nation-states) and micro-elements (such as behavioral economic insights into how people understand and interact with security features). Specific topics include policymaking, business models, legal frameworks, national security considerations, ethical issues, standards making, and the roles of users, government, and industry.

Beyond the Code: Cybersecurity in Context: Read More [+]

Rules & Requirements

Prerequisites: MICS students only

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W200

Beyond the Code: Cybersecurity in Context: Read Less [-]

CYBER 202 Cryptography for Cyber and Network Security 3 Units

Terms offered: Not yet offered
This course focuses on both mathematical and practical foundations of cryptography. The course discusses asymmetric and symmetric cryptography, Kerchkoff's Principle, chosen and known plaintext attacks, public key infrastructure, X.509, SSL/TLS (https), and authentication protocols. The course will include an in-depth discussion of many different cryptosystems including the RSA, Rabin, DES, AES, Elliptic Curve, and SHA family cryptosystems. This course also introduces advanced topics of applied cryptography, including a brief introduction to homomorphic encrypted computation and secure multi-party computation to protect sensitive data during arbitrary computation, cryptocurrency and its cryptographic building blocks, and quantum computing.
Cryptography for Cyber and Network Security: Read More [+]
Rules & Requirements

Prerequisites: MICS students only

Credit Restrictions: Students will receive no credit for CYBER W202 after completing CYBER 202. A deficient grade in CYBER W202 may be removed by taking CYBER 202.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W202

Cryptography for Cyber and Network Security: Read Less [-]

CYBER 204 Software Security 3 Units

Terms offered: Not yet offered
The course presents the challenges, principles, mechanisms and tools to make software secure. We will discuss the main causes of vulnerabilities and the means to avoid and defend against them. The focus is on secure programming practice, including specifics for various languages, but also covering system-level defenses (architectural approaches and run-time enforcement). We will also apply software analysis and vulnerability detection tools in different scenarios.
Software Security: Read More [+]
Objectives & Outcomes

Course Objectives: *Apply and manage secure coding practices throughout software project development

*Gain a good comprehension of the landscape of software security vulnerabilities, with specifics for various programming languages and types of software applications

*Gain the ability to analyze the security of a software system and convincingly advocate about the significance of vulnerabilities

*Know representative tools for software security analysis and testing, use them in practice and understand their capabilities and limitations

*Recognize insecure programming patterns and know how to replace them with secure alternatives

Student Learning Outcomes: Students will be able to apply and manage secure coding practices throughout software project development
Students will be able to recognize insecure programming patterns and know how to replace them with secure alternatives
Students will gain a good comprehension of the landscape of software security vulnerabilities, with specifics for various programming languages and types of software applications
Students will gain the ability to analyze the security of a software system and convincingly advocate about the significance of vulnerabilities
Students will know representative tools for software security analysis and testing, use them in practice and understand their capabilities and limitations

Rules & Requirements

Prerequisites: MICS students only. CYBER W202 must be taken prior to or concurrently with CYBER W204. Knowledge of at least one non-scripting programming language (e.g. C, C++, or Java); fundamental knowledge of information systems (review of operating systems notions)

Credit Restrictions: Students will receive no credit for CYBER W204 after completing CYBER 204. A deficient grade in CYBER W204 may be removed by taking CYBER 204.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W204

Software Security: Read Less [-]

CYBER 206 Programming Fundamentals for Cybersecurity 3 Units

Terms offered: Not yet offered

This course is designed to provide students with the foundational math and programming skills required to be successful in the Master of Information and Cybersecurity (MICS) program. Upon completion of this course, students will be able to write programs in Python and will gain experience reading and interpreting C programs. Students will receive a comprehensive overview of algebraic principles and will explore quantitative concepts needed for cryptography. Additionally, this course will prepare students to apply logical thinking and decompose complex problems to create programmatic solutions.

Programming Fundamentals for Cybersecurity: Read More [+]

Rules & Requirements

Prerequisites: MICS students only

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W206

Programming Fundamentals for Cybersecurity: Read Less [-]

CYBER 207 Applied Machine Learning for Cybersecurity 3 Units

Terms offered: Not yet offered

Machine learning is a rapidly growing field at the intersection of computer science and statistics concerned with finding patterns in data. It is responsible for tremendous advances in technology, from personalized product recommendations to speech recognition in cell phones. This course provides a broad introduction to the key ideas in machine learning, with a focus on applications and concepts relevant to cybersecurity. The emphasis will be on intuition and practical examples rather than theoretical results, though some experience with probability, statistics, and linear algebra will be important.

Applied Machine Learning for Cybersecurity: Read More [+]

Rules & Requirements

Prerequisites: MICS students only. Experience with probability and statistics. Intermediate competency in Python, C, or Java, and competency in Linux, GitHub, and relevant Python libraries; or permission of instructor. Linear algebra is recommended

Credit Restrictions: Students will receive no credit for CYBER W207 after completing CYBER 207. A deficient grade in CYBER W207 may be removed by taking CYBER 207.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W207

Applied Machine Learning for Cybersecurity: Read Less [-]

CYBER 210 Network Security 3 Units

Terms offered: Not yet offered
Introduction to networking and security as applied to networks. Exercises cover network programming in a language of the student's choice, understanding and analyzing packet traces using tools like wireshark and mitmproxy, as well as applying security principles to analyze and determine network security. After this course, the student will have a fundamental understanding of networking, TLS and security as it applies to networked systems.
Network Security: Read More [+]
Rules & Requirements

Prerequisites: MICS students only. Basic understanding of internet network protocols

Credit Restrictions: Students will receive no credit for CYBER W210 after completing CYBER 210. A deficient grade in CYBER W210 may be removed by taking CYBER 210.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W210

Network Security: Read Less [-]

CYBER 211 Operating System Security 3 Units

Terms offered: Not yet offered
This survey of operating system security compares approaches to security taken among several modern operating systems. The course will teach how to conceptualize design issues, principles, and good practices in securing systems in today’s increasingly diverse and complex computing ecosystem, which extends from things and personal devices to enterprises, with processing increasingly in the cloud. We will approach operating systems individually and then build on them so that students learn techniques for establishing trust across a set of interoperating systems.
Operating System Security: Read More [+]
Rules & Requirements

Prerequisites: CYBER W200, CYBER W202, CYBER W204, and CYBER W210. Working knowledge of at least one object-oriented programming language and computer architecture (e.g. Intel x86-64bit). MICS students only

Credit Restrictions: Students will receive no credit for CYBER W211 after completing CYBER 211. A deficient grade in CYBER W211 may be removed by taking CYBER 211.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W211

Operating System Security: Read Less [-]

CYBER 215 Usable Privacy and Security 3 Units

Terms offered: Not yet offered
Security and privacy systems can be made more usable by designing them with the user in mind, from the ground up. In this course, you will learn many of the common pitfalls of designing usable privacy and security systems, techniques for designing more usable systems, and how to evaluate privacy and security systems for usability. Through this course, you will learn methods for designing software systems that are more secure because they minimize the potential for human error.
Usable Privacy and Security: Read More [+]

Rules & Requirements

Prerequisites: MICS students only. CYBER W200, CYBER W202

Credit Restrictions: Students will receive no credit for CYBER W215 after completing CYBER 215. A deficient grade in CYBER W215 may be removed by taking CYBER 215.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W215

Usable Privacy and Security: Read Less [-]

CYBER 220 Managing Cyber Risk 3 Units

Terms offered: Not yet offered
This course offers valuable perspective for both the non-technical business manager and the technical cybersecurity or IT manager. It is the vital connector between the technical world of threats, vulnerabilities, and exploits, and the business world of board-level objectives, enterprise risk management, and organizational leadership. Now more than ever, managers have a need and responsibility to understand cyber risk.
Just as financial risks and other operational risks have to be effectively managed within an organization, cyber risk has to be managed. It spans far beyond information technology, with broad implications in the areas of organizational behavior, financial risk modeling, legal issues, and executive leadership.
Managing Cyber Risk: Read More [+]

Objectives & Outcomes

Student Learning Outcomes: Compare and employ approaches to cyber risk management and measurement.
Develop a basic cybersecurity strategic plan and understand how it aligns with the core business value of the company.
Navigate corporate structures to create a strong cyber security program and obtain senior leadership buy-in.
Understand security product verticals, identify common use cases for those products, and define requirements for acquiring solutions relevant to a business use case.
Understand the basic principles and best practices of responding to a cybersecurity incident

Rules & Requirements

Prerequisites: MICS students only

Credit Restrictions: Students will receive no credit for CYBER W220 after completing CYBER 220. A deficient grade in CYBER W220 may be removed by taking CYBER 220.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W220

Managing Cyber Risk: Read Less [-]

CYBER 233 Privacy Engineering 3 Units

Terms offered: Not yet offered

This course surveys privacy mechanisms applicable to systems engineering, with a particular focus on the inference threat arising due to advancements in artificial intelligence and machine learning. We will briefly discuss the history of privacy and compare two major examples of general legal frameworks for privacy from the United States and the European Union. We then survey three design frameworks of privacy that may be used to guide the design of privacy-aware information systems. Finally, we survey threat-specific technical privacy frameworks and discuss their applicability in different settings, including statistical privacy with randomized responses, anonymization techniques, semantic privacy models, and technical privacy mechanisms.

Privacy Engineering: Read More [+]

Objectives & Outcomes

Student Learning Outcomes: Students should be able to implement such privacy paradigms, and embed them in information systems during the design process and the implementation phase.

Students should be familiar with the different technical paradigms of privacy that are applicable for systems engineering.

Students should develop critical thinking about the strengths and weaknesses of the different privacy paradigms.

Students should possess the ability to read literature in the field to stay updated about the state of the art.

Rules & Requirements

Prerequisites: MICS students only; or, permission of instructor

Credit Restrictions: Students will receive no credit for CYBER W233 after completing CYBER 233. A deficient grade in CYBER W233 may be removed by taking CYBER 233.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W233

Privacy Engineering: Read Less [-]

CYBER 242 Government, National Security, and the Fifth Domain 3 Units

Terms offered: Not yet offered

A variety of actors exploit government and private networks, systems, and data. Perpetrators target these systems to engage in cybercrime, espionage, disinformation campaigns, disruption of essential services, destruction of critical infrastructure, and the deletion, theft, or alteration of data. The government, military, and private sector have various roles and responsibilities with regard to the protection of the cyber domain. In this course, students critically evaluate these roles and responsibilities, the manner in which government networks, systems, and data are secured, and the ability of national and international cybersecurity strategies and partnerships to provide effective and efficient protection of the fifth domain.

Government, National Security, and the Fifth Domain: Read More [+]

Objectives & Outcomes

Student Learning Outcomes: Critically assess national and international cybersecurity strategies

Describe and evaluate national and international public-private partnerships.

Discuss the fifth domain and its protection within the context of national security.

Identify lessons learned and recommend ways to improve national and international approaches to cybersecurity.

Identify the roles and responsibilities of the military, government, and the private sector in cybersecurity.

Utilize an evidence-based approach to analyze the security of government networks and systems and privacy of retained data.

Rules & Requirements

Prerequisites: MICS students only. CYBER W200, CYBER W202

Credit Restrictions: Students will receive no credit for CYBER W242 after completing CYBER 242. A deficient grade in CYBER W242 may be removed by taking CYBER 242.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Formerly known as: Information and Cybersecurity W242

Government, National Security, and the Fifth Domain: Read Less [-]

CYBER W289 Public Interest Cybersecurity: The Citizen Clinic Practicum 3 Units

Terms offered: Spring 2022, Fall 2021, Summer 2021
This course provides students with real-world experience assisting politically vulnerable organizations and persons around the world to develop and implement sound cybersecurity practices. In the classroom, students study basic theories and practices of digital security, intricacies of protecting largely under-resourced organizations, and tools needed to manage risk in complex political, sociological, legal, and ethical contexts. In the clinic, students work in teams supervised by Clinic staff to provide direct cybersecurity assistance to civil society organizations. We emphasize pragmatic, workable solutions that take into account the unique needs of each partner organization.
Public Interest Cybersecurity: The Citizen Clinic Practicum: Read More [+]

Rules & Requirements

Prerequisites: Master of Information and Cybersecurity students only

Hours & Format

Summer: 14 weeks - 6 hours of clinic and 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Instructor: Weber

Public Interest Cybersecurity: The Citizen Clinic Practicum: Read Less [-]

CYBER 290 Special Topics 3 Units

Terms offered: Fall 2021
Specific topics, may vary from section to section, year to year.
Special Topics: Read More [+]

Rules & Requirements

Prerequisites: MICS students only

Repeat rules: Course may be repeated for credit when topic changes. Students may enroll in multiple sections of this course within the same semester.

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of lecture per week

Summer: 14 weeks - 3 hours of lecture per week

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Special Topics: Read Less [-]

CYBER W295 Capstone 3 Units

Terms offered: Spring 2022, Fall 2021, Summer 2021
This capstone course will cement skills and knowledge learned throughout the Master of Information and Cybersecurity program: core cybersecurity technical skills, understanding of the societal factors that impact the cybersecurity domain and how cybersecurity issues impact humans, and professional skills such as problem-solving, communication, influencing, collaboration, and group management – to prepare students for success in the field. The centerpiece is a semester-long group project in which teams of students propose and select a complex cybersecurity issue and apply multi-faceted analysis and problem-solving to identify, assess, and manage risk and deliver impact.
Capstone: Read More [+]

Objectives & Outcomes

Student Learning Outcomes: Engage in a highly collaborative process of idea generation, information sharing, and feedback that replicates key aspects of managing cybersecurity in an organizational setting.
Learn or reinforce communication, influencing, and management skills.
Practice using multi-faceted problem-solving skills to address complex cybersecurity issues.

Rules & Requirements

Prerequisites: CYBER W200, CYBER W202, and CYBER W204. MICS students only. Must be taken in final term of the MICS program

Hours & Format

Fall and/or spring: 14 weeks - 3 hours of web-based lecture per week

Summer: 14 weeks - 3 hours of web-based lecture per week

Online: This is an online course.

Additional Details

Subject/Course Level: Information and Cybersecurity/Graduate

Grading: Letter grade.

Capstone: Read Less [-]