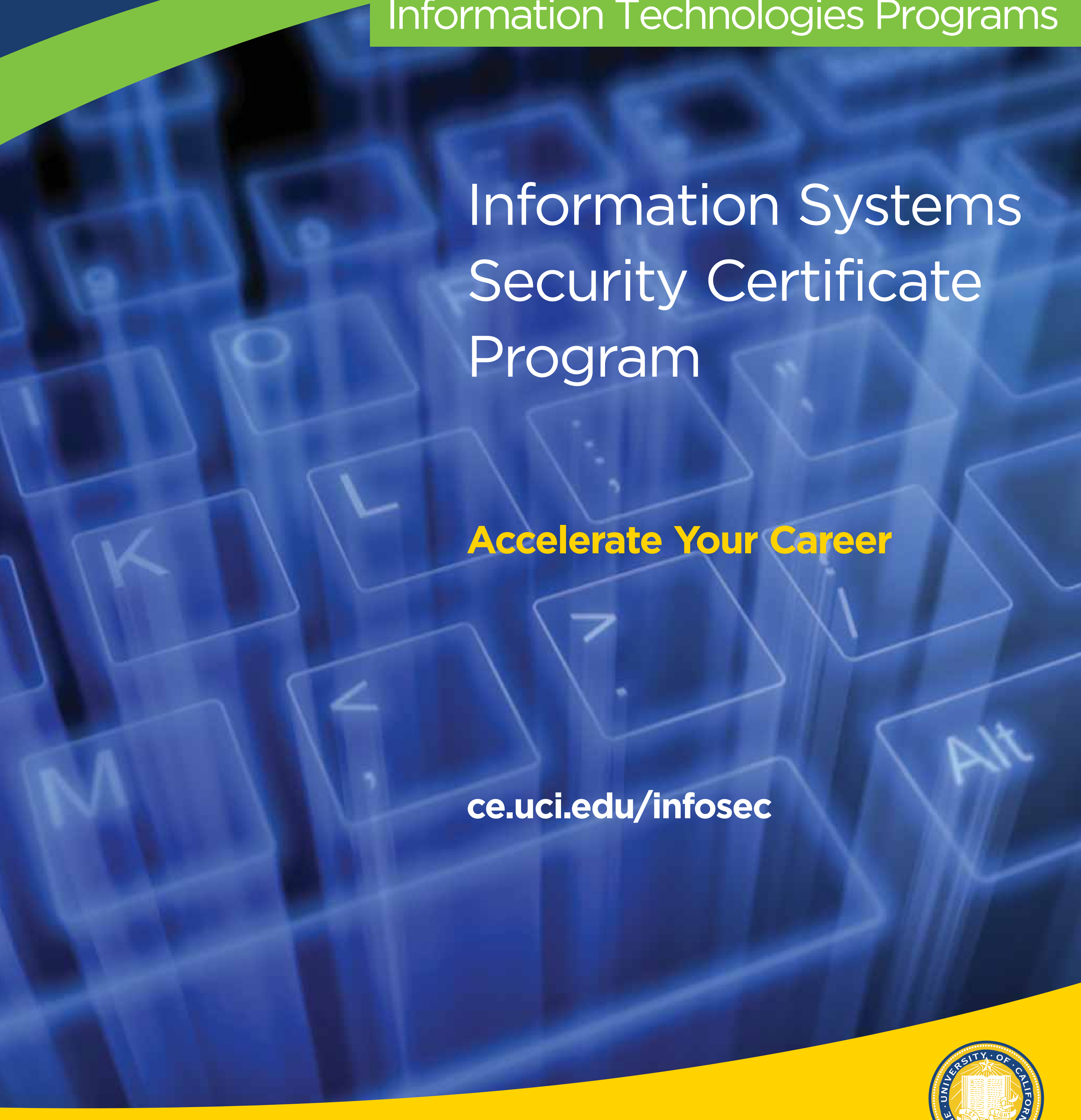
UCI Division of
Continuing Education

Information Technologies Programs



Information Systems Security Certificate Program

Accelerate Your Career

ce.uci.edu/infosec

University of California, Irvine

Improve Your Career Options with a Professional Certificate

UCI Division of Continuing Education's professional certificate and specialized studies programs help you increase or enhance your current skills or prepare for a new career. Courses are highly practical and instructors are qualified leaders in their field. Convenient online courses make it easy to learn on your own time, in your own way. A certificate bearing the UC seal signifies a well-known, uncompromising standard of excellence.

Information Systems Security Certificate Program

Corporations have been put on alert to heighten their infrastructure and data security due to threats from hackers and cyber-terrorists. As information security threats and high visibility breaches have skyrocketed in the past few years, government agencies and customers have dramatically increased their requirements and scrutiny of corporate security process and procedures. UCI Continuing Education's Certificate program in Information Systems Security prepares professionals within a wide range of career levels to develop the skills they need to succeed in this rapidly expanding, dynamic field.

The curriculum focuses on developing a comprehensive understanding of the underlying principles for designing, engineering, and managing secure information systems environments. Core topic areas include: access control; application development security; business continuity; disaster recovery planning; cryptography; information security governance; risk management; legal; regulations; investigations and compliance; operations security; physical (environmental) security; security architecture; design and telecommunications; and network security. Learn how to effectively combat external attacks that can compromise data and business operations through our cyber security track of elective courses. This program will help prepare you to sit for the Certified Information Systems Security Professional (CISSP®) exam administered by the International Information Systems Security Certification Consortium, Inc., (ISC)²®.

For More Information:
Julie Pai
Program Representative
julie.pai@uci.edu
(949) 824-6333

Who Should Enroll?

This program has been designed to benefit security professionals who require CISSP® certification and work on software development and information technology infrastructure teams, security technicians working with Internet service providers, application service providers, systems integrators, and security auditors. Business professionals who must combat potential cyber-threats and attacks that endanger their organizations' data will also benefit from this program.

The program also includes courses that expand technical skills and enable security professionals and those training to be security professionals to pursue and maintain a variety of industry certifications. The courses include current findings from academic and technological research and state-of-the-art practice.

Program Benefits:

- Develop key knowledge of information systems security, including access control, administration, audit and monitoring, risk, response, and recovery
- Protect the confidentiality, integrity, and availability (CIA) of stored information
- Implement government and customer imposed security requirements
- Develop best practices for business continuity planning
- Broaden your knowledge to include the implementation of multiple technologies, including client/server, Web, mainframe, and wireless
- Identify and apply industry standards at the physical, personal, and organizational level
- Design, diagnose, implement, manage, and resolve complex computer security threats
- Gain the knowledge required to obtain your CISSP® certification.

Program Fees

Course Fees:	$5,075
Candidacy Fee:	$ 125
Textbooks and Materials:	$ 700
Total Estimated Cost:	$5,900

Certificate Requirements

A certificate is awarded upon completion of 15 credit untis (3 required and 6 elective credit units) with a grade point average of ‘B’ or better.

To become an official candidate in the program, students pursuing the certificate must submit a **Declaration of Candidacy**. To receive the certificate after completing all program requirements, students must submit a **Request for Certificate**. All requirements must be completed within 5 years after the student enrolls in his/her first course. Students not pursuing the certificate program are welcome to take as many individual courses as they wish.

Transfer Credit

Graduates from UCI Continuing Education’s Information Systems Security Certificate program are eligible to transfer credits to University of Wisconsin-Platteville, Master of Science in Criminal Justice and University of Maryland, Baltimore County (UMBC), Master in Professional Studies (MPS): Cybersecurity programs.

Onsite Training

Our Corporate Training specialists can deliver this program or a customized one that fits your organization’s specific needs. Visit ce.uci.edu/corporte or call (949) 824-1847 for information.

Complete Certificate Program Online

Curriculum

Required Courses

Introduction to Information Systems Security

I&C SCI X465.00 (3 units)

Focuses on basic computer security concepts as they pertain to logical and physical security at corporate or remote arenas including mobile workforce. This introductory course will expose students to various design principles of trusted computing bases, legal regulations, investigation and compliance requirements, secure computing concepts, numerous security protocols and principles, practical networking security methodologies. An introduction to business continuity and disaster recovery concepts will also be discussed.

Secure Systems

I&C SCI X465.01 (3 units)

This course will focus on design principles of trusted computing bases (TCB). Issues regarding authentication, access control and authorization, introductory cryptography, controls categories, media, backups and change control management, discretionary and mandatory security policies, secure kernel design, application development security, secure operating systems (patching and vulnerability management), and secure databases will be covered from a systems architecture perspective. Emphasis will be on the design of security measures for critical information infrastructures.

Security Architecture & Design

I&C SCI X465.02 (3 units)

Learn the fundamentals of security architecture design including security models, enterprise architecture and security evaluations. Understand critical issues related to network security such as the OSI reference model, firewalls, TCP/IP and LAN. Apply techniques used to support larger networks such as MAN and WAN, and those accessed via wireless protocols. Discover the practical aspects of cryptography concepts and how to apply them to improve the security of information systems.

Elective Courses (Choose 6 units)

Host and OS Security

I&C SCI X465.03 (1.5 units)

This course will focus on the security aspects of Windows Vista, MAC, and Apple OS technology as it applies to the home and mobile user configuration. It will also cover the various networking and standalone OS's that are prominent in the corporate world and vital to any company's client-to-server operations as well as information security governance and risk management.

Database Security

I&C SCI X465.05 (3 units)

Covers issues related to the design and implementation of secure data stores. Emphasis will be placed on multilevel security in database systems, covert channels, and security measures for relational and object-oriented database systems.

Network Security: Concepts & Technologies

I&C SCI X465.06 (3 units)

Fundamental concepts, principles, networking and inter-networking issues relevant to the design, analysis, and implementation of enterprise-level networked systems are covered in this course. Topics include networking and security architectures, techniques, and protocols at the various layers of the Internet model. Security problems will be analyzed, discussed, and implemented.

Cyber Security Track

Introduction to Computer Forensics

I&C SCI X465.07 (3 units)

Designed to provide a solid foundation in the theory and practice of essential computer forensic techniques, this introductory course in computer forensics focuses on preparing students to respond to many types of crisis situations by providing the skills needed to respond to an investigation. Focus is placed on the role of computer forensics and the methods used in the investigation of computer crimes. Other topics covered include aspects of the legal process that apply to computer forensics, detailed explanations of how to effectively manage a forensics investigation, and ways to preserve and present evidence. On the technical side, forensics on Windows Systems including the file system, the registry, and events will be discussed. Live analysis, linux systems, and browser artifacts are also included in the topics covered along with a primer on commercial tools as well as open source tools available.

Reverse Engineering

I&C SCI X465.10

Understanding and analyzing malware through the process of reverse engineering is a key methodology to stop malware attacks. Learn how to use this process to discover vulnerabilities in binaries in order to properly secure your organization from ever evolving threats. This class covers a wide variety of malware, from native Windows executables, to web-based malware with numerous types of obfuscation. Take a hands-on approach to learn how to reverse-engineer malicious code using system/network monitoring utilities, debuggers, disassemblers, and a handful of scripts.

Advisory Committee

Leo A. Dregier III, CISSP®, CEH™, CHFI™, CISM®, CEO, The Security Matrix, LLC

Nelson Eby, M.S., ACE, Forensic Analyst, GE, Federal Bureau of Investigation CART, Member of Technical Working Group for Education and Training in Computer Forensics

Tony Gaidhane, MBA, M.S., CISSP(r), CISM(r), CISA(r), PMP, Director, Identity Management, WellPoint Inc.

Ian Harris, Ph.D., Associate Professor, Donald Bren School of Information and Computer Science, University of California, Irvine

Terry House, Ph.D., Assistant Professor of Computer Science, Methodist University

Barbara Johnson, CISA®, CISSP®, ISSMP®, CBCP, MBCI, Information Security and Business Continuity Consultant, Member of the (ISC)^2® Common Body of Knowledge (CBK) Committee

Caitlin Pantos, Senior Program Manager, Privacy & Security, Google Inc.

David M. Mahoney, MBA, CISSP®, PMP®, Manager Infrastructure Services, Information Systems Sector, Civil Systems Division, Northrop Grumman Corporation

Pramod Pandya, Ph.D., Professor and Director, Information Technologies, California State University Fullerton

Debbie Rodriguez, MBA, CISSP®, CISA®, System Analyst, Intuit Financial Services

Maria Suarez, Chief Information Security Officer, University of Southern California

Academic Management

Dave Dimas, Ph.D., Director, Engineering, Sciences and Information Technologies

Information Systems Security Certificate Program

Julie Pai ▪ (949) 824-6333 ▪ julie.pai@uci.edu

UCI Division of Continuing Education

09.22.16

ce.uci.edu/infosec