Hochschule
Albstadt-Sigmaringen
Albstadt Sigmaringen University

Study Abroad - Certificate in IT Security

30 ECTS credit program

Program Modules:

Module	ECTS
Compulsory modules:	
Digital Forensics	5
Cybersecurity Awareness and Behavior	5
Introduction to Cyberpsychology	2,5
Project in Computing	7,5
Offensive Security Measures	7,5
Choice option (choose one):	
IT Security Management	2,5
Mobile and Cloud Forensics	2,5

Further Information / Contact:

International Office
Albstadt- Sigmaringen University
Dr. Conny Bast
bast@hs-albsig.de

International relations
Study Abroad Certificate in IT Security
Prof. Dr. Stefan Sütterlin
suetterlin@hs-albsig.de

Study Abroad Certificate in IT Security
Module: Digital Forensics

Key facts

Workload		**ECTS**
150 h		5
Parts of the module	**Contact time**	**Self-study time**
	60 h	90 h
Module leader	**Assessment**	
Prof. Holger Morgenstern	Oral exam	

Curriculum Outline

The students

- are familiar with the methodological foundation of digital forensics and its embedding in classical analogue forensics
- understand forensic principles in securing and analyzing digital traces
- can document and present the forensic examinations, e.g. in court
- are able to apply the techniques learned in various areas of digital forensics (e.g., disk forensics, application forensics, digital forensics, mobile devices)

Key content

- Introduction to forensic sciences in general and digital forensics in particular
- Methodical foundation of digital forensics, embedded in classical analogue forensics
- Forensic principles in securing and analyzing digital spotting and presentation of forensic investigations (internally and in court)
- Practical applications in various areas of digital forensics (e.g., disk forensics, application forensics, digital forensics, mobile devices)

Study Abroad Certificate in IT Security

Module: Cybersecurity Awareness and Behaviour

Key facts

Workload		**ECTS**
150 h		5
Parts of the module	**Contact time**	**Self-study time**
	60 h	90 h
Module leader	**Assessment**	
Prof. Dr. Stefan Sütterlin	Presentation & home work	

Curriculum Outline

The "Cybersecurity Awareness and Behavior" module thoroughly explores the facets of cybersecurity awareness training tailored to corporate and organizational environments.

Key content

The course begins by introducing students to various training formats and designs that meet diverse organizational needs. It then delves into methods for evaluating the effectiveness of these cybersecurity trainings, with a particular focus on their impact on organizational security. The curriculum further guides students through the statistical techniques and methodological approaches that are essential for analyzing and evaluating the outcomes of cybersecurity education. Emphasis is also placed on creating employee-centered and adaptive interventions, designed to cater specifically to the needs and behaviors of employees to enhance cybersecurity practices effectively. Additionally, the course covers the exploration of cybersecurity culture within organizations and the practices of cyberhygiene necessary to maintain secure operations. Another significant aspect of the module is the development and design of self-report assessments, including surveys and questionnaires, which are crucial for measuring the awareness and effectiveness of cybersecurity initiatives. Students also examine the critical success factors that influence the effectiveness of sensitizing efforts towards cybersecurity threats and best practices. The course concludes by addressing various behavior change models and strategies to ensure the sustainability of training effects, ultimately aiming to enhance long-term cybersecurity behavior within organizations. Overall, this module is designed to equip students with the necessary skills and knowledge to effectively plan, implement, and evaluate comprehensive cybersecurity awareness programs across various organizational contexts.

Study Abroad Certificate in IT Security
Module: Introduction to Cyberpsychology

Key facts

Workload		**ECTS**
75 h		2,5
Parts of the module	**Contact time**	**Self-study time**
	15 h	52,5 h
Module leader	**Assessment**	
Prof. Dr. Stefan Sütterlin	Written exam	

Curriculum Outline

The module "Introduction to Cyberpsychology" discusses a variety of aspects in the area of human perception, emotions, decision-making and other aspects of behavior in the context of cyberspace and online worlds. The module is of interest for students of all areas where the interaction of humans with computers plays a role. No previous knowledge of IT Security or psychology is required.

Key content

Examples for topic areas covered in the module are:
- Gaming, Games and Gamification
- The human factor in IT-Security
- Cybercrime and cyber defense
- Dark Patterns, Usability, and manipulation via user interfaces
- Bio-psychological aspects of human-computer interaction (e.g. brain-computer interfaces)
- Cognitive aspects of deep fake recognition
- Generation, spread and effects of political disinformation in cyberspace
- Trust in automation and human-robot-interaction

Study Abroad Certificate in IT Security

Module: Project in Computing

Key facts

Workload		**ECTS**
225 h		7,5
Parts of the module	**Contact time**	**Self-study time**
Project 4 SWS, Seminar 2 SWS	90h	135 h
Module leader	**Assessment**	
Prof. Dr. Bernd Stauß	Project work, homework	

Curriculum Outline

Independent work on a real project with the topic out of the study area, from problem analysis until the final product. This happens in a group.
Teams are guided by a professor and teaching assistants.

Key content

Content depends on the topic of the project.

Study Abroad Certificate in IT Security
Module: Offensive Security Measures

Key facts

Workload		ECTS
225 h		7,5
Parts of the module	Contact time	Self-study time
Seminar + practical training	90 h	135 h
Module leader	Assessment	
Prof. Dr. Bernhard Jungk	Presentation, report, practical training results	

Curriculum Outline

Students will get broad knowledge of offensive methods of IT security including PEN tests, CIA attacks on systems, networks and communication channels, in-depth knowledge of current offensive tools and frameworks, including current Metasploit.
They will be able to penetrate protected IT systems using extensive and diverse offensive methods and tools to penetrate protected IT systems. They will also be able to develop and apply new offensive tools and scripts and assess the level of security from the results of offensive security tests.

Key Content

- Offensive methods and their goals in the context of IT security
- Legal and Ethical Framework
- Fundamentals, framework conditions and goals of penetration tests
- Attacks on the confidentiality, integrity or availability of
  >transmission channels
  >networks
  >operating systems
  >Applications
  >Hardware components
  >Web applications
  >radio systems
- Finding vulnerabilities through fuzzing and code analysis

Laboratory work: The points dealt with in the lecture are practically tested in the lab within an isolated network. Current tools and systems from the penetration test and system analysis area such as Burp Suite, Nmap, and the Metasploit Framework.

Study Abroad Certificate in IT Security
Choice Module 1: IT Security Management

Key facts

Workload		**ECTS**
75 h		2,5
Parts of the module	**Contact time**	**Self-study time**
	30 h	45 h
Module leader	**Assessment**	
Prof. Holger Morgenstern / Hr. Wagner	Written exam	

Curriculum Outline

Students receive broad knowledge of the basics and importance of IT security management, in-depth knowledge of relevant standards and regulations in the field of IT security management.
Students are proficient in a broad range of methods and tools for the design and implementation of an ISM, students are able to assess the IT security level of an organization at the organizational level and to improve it by means of ISM
The security level and security risks of corporate IT can be critically assessed with regard to critically reflect on the legal and ethical framework.

Key content

- Fundamentals and significance of IT security management
- Legal requirements
- IT security standards
- IT security management process
- IT security management according to BSI basic protection
- Standards and certification
- Organizational aspects

Study Abroad Certificate in IT Security
Choice Module 2: Mobile and Cloud Forensics

Key facts

Workload		ECTS
75 h		2,5
Parts of the module	Contact time	Self-study time
	30 h	45 h
Module leader	Assessment	
Prof. Dr. Christofer Fein	Written exam	

Curriculum outline

Students gain a broad knowledge of forensic methods, specializing in the mobile and cloud area. They will learn a wide range of forensic methods for securing and analyzing digital securing and analyzing digital traces in the mobile and cloud area.

Students are able to assess the possibilities and limits of the forensic methods and tools they have learned and to expand these and develop new scripts/tools.

Students can assess the relevance and security of secured and analyzed digital traces.

Key Content

- Digital forensics in the context of mobile devices (smartphones, navigation devices, etc.)
- Special features in the area of forensic backup and analysis of mobile devices (operating systems, file systems, data formats, access options and restrictions)
- Digital forensics in the context of cloud computing
- Special features in the area of forensic protection and analysis of cloud systems (architectures, service and organizational models, trust models, access options and restrictions)
- Practical applications and exercises in digital forensics of mobile devices and cloud systems