ITR - IT-Security, IT-Recht und Datenschutz

ITR - IT-Security, IT-Law and Data Privacy

General information	
Module Code	ITR
Unique Identifier	ITSecITRDatB-01-BA-M
Module Leader	Prof. Dr. Kürtz, Klaas Ole (klaas.o.kuertz@haw-kiel.de)
Lecturer(s)	Prof. Dr. Kürtz, Klaas Ole (klaas.o.kuertz@haw-kiel.de) Prof. Dr. Stark, Thorsten (thorsten.stark@haw-kiel.de)
Offered in Semester	Wintersemester 2026/27
Module duration	1 Semester
Occurrence frequency	Regular
Module occurrence	In der Regel im Wintersemester
Language	Deutsch
Recommended for international students	Yes
Can be attended with different study programme	No

Curricular relevance (according to examination regulations)
Study Subject: B.Sc. - WINF 7 Sem. - Wirtschaftsinformatik (7 Sem.) Module type: Pflichtmodul Semester: 5

Qualification outcome
Areas of Competence: Knowledge and Understanding; Use, application and generation of knowledge; Communication and cooperation; Scientific self-understanding / professionalism.
Die Studierenden verstehen die grundlegenden Aspekte des Managements der Cybersicherheit und der digitalen Resilienz. Sie kennen die Grundkonzepte von Angreifermodellen und verstehen im Ansatz die Funktionsweise verschiedener Angriffstechniken. Sie kennen Grundlagen der Kryptographie, ausgewählte Sicherheitsmechanismen, und Systematik von möglichen Schutzmaßnahmen. Sie verstehen die Notwendigkeit für und die Kernelemente von verschiedenen Ansätzen zur Sicherstellung der betrieblichen Kontinuität im Ereignisfall. Die Studierenden kennen grundsätzlich die von IT-Recht und Datenschutz betroffenen Themenfelder.
Die Studierenden können Ebenen der Cybersicherheit im Kontext von Unternehmen oder Organisationen anwenden, inklusive mathematisch-kryptographischer Grundlagen, technischer Maßnahmen, organisatorischer und strategischer Maßnahmen, Elementen menschlichen Verhaltens sowie rechtlichen Aspekten. Die Studierenden sind in der Lage, eigene Analysen zur Cybersicherheit im betrieblichen Umfeld durchzuführen und die Ergebnisse geeignet zu dokumentieren. Sie besitzen erste Kompetenzen zur Durchführung einer Risikobewertung.
Die Studierenden können Problemstellungen der Cybersicherheit und des IT-Rechts erörtern und diskutieren. Die Studierenden können selbst erarbeitete Inhalte mit Bezug zu Cybersicherheit, digitaler Resilienz und IT-Recht verständlich und überzeugend aufbereiten und präsentieren, sowie inhaltliche Aspekte sachgerecht und fachlich kompetent diskutieren. Sie können kompetent einschätzen, wann rechtliche Fragestellungen das Einbeziehen von Expert*innen erfordert.

Content information	
Content	Grundlagen der Cybersicherheit, Informationssicherheit, IT-Sicherheit, digitalen Resilienz Angreifermodelle und Bedrohungen, Angriffstechniken Schutzziele, Schutz- und Gegenmaßnahmen zur Sicherung von Daten, IT-Systemen und Organisationen Grundlagen der angewandten Kryptographie und des Risiko- und Krisenmanagements Grundlagen im IT-Recht inklusive Datenschutz #cybersicherheit #itsicherheit #digitaleresilienz #angriffsvektoren #angriffsmethoden #risikomanagement #dsgvo
Literature	Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems Wiley; 2. edition (April 14, 2008) ISBN-13: 978-0470068526 Online verfügbar unter http://www.cl.cam.ac.uk/~rja14/book.html Matt Bishop: Computer Security – Art and Science Addison-Wesley Professional; 1. edition (December 12, 2002) ISBN-13: 978-0201440997 Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C Wiley; 2. edition (November 2, 1995) ISBN-13: 978-0471128458

Courses

Mandatory Courses

For this module all specified courses in the following table have to be taken.

ITRD - IT-Recht und Datenschutz - Page: 6
ITS - IT-Security - Page: 4

Workload	
Number of SWS	4 SWS
Credits	5,00 Credits
Contact hours	48 Hours
Self study	102 Hours

Module Examination	
Examination prerequisites according to exam regulations	None
ITR - Klausur	Method of Examination: Klausur Duration: 60 Minutes Weighting: 50% wird angerechnet gem. § 11 Absatz 2 PVO: No Graded: Yes Remark: IT-Security

ITR - Präsentation	Method of Examination: Präsentation Duration: 30 Minutes Weighting: 50% wird angerechnet gem. § 11 Absatz 2 PVO: No Graded: Yes Remark: IT-Recht und Datenschutz

Course: IT-Security

General information	
Course Name	IT-Security IT-Security
Course code	ITS
Lecturer(s)	Prof. Dr. Kürtz, Klaas Ole (klaas.o.kuertz@haw-kiel.de)
Occurrence frequency	Regular
Module occurrence	In der Regel im Wintersemester
Language	Deutsch

Qualification outcome
Areas of Competence: Knowledge and Understanding; Use, application and generation of knowledge; Communication and cooperation; Scientific self-understanding / professionalism.
Die Studierenden verstehen die grundlegenden Aspekte des Managements der Cybersicherheit und der digitalen Resilienz. Sie kennen die Grundkonzepte von Angreifermodellen und verstehen im Ansatz die Funktionsweise verschiedener Angriffstechniken. Sie kennen Grundlagen der Kryptographie, ausgewählte Sicherheitsmechanismen, und Systematik von möglichen Schutzmaßnahmen. Sie verstehen die Notwendigkeit für und die Kernelemente von verschiedenen Ansätzen zur Sicherstellung der betrieblichen Kontinuität im Ereignisfall. Die Studierenden kennen grundsätzlich die von IT-Recht und Datenschutz betroffenen Themenfelder.
Die Studierenden können Ebenen der Cybersicherheit im Kontext von Unternehmen oder Organisationen anwenden, inklusive mathematisch-kryptographischer Grundlagen, technischer Maßnahmen, organisatorischer und strategischer Maßnahmen, Elementen menschlichen Verhaltens sowie rechtlichen Aspekten. Die Studierenden sind in der Lage, eigene Analysen zur Cybersicherheit im betrieblichen Umfeld durchzuführen und die Ergebnisse geeignet zu dokumentieren. Sie besitzen erste Kompetenzen zur Durchführung einer Risikobewertung.
Die Studierenden können Problemstellungen der Cybersicherheit und des IT-Rechts erörtern und diskutieren. Die Studierenden können selbst erarbeitete Inhalte mit Bezug zu Cybersicherheit, digitaler Resilienz und IT-Recht verständlich und überzeugend aufbereiten und präsentieren, sowie inhaltliche Aspekte sachgerecht und fachlich kompetent diskutieren. Sie können kompetent einschätzen, wann rechtliche Fragestellungen das Einbeziehen von Expert*innen erfordert.

Content information	
Content	Grundlagen der Cybersicherheit, Informationssicherheit, IT-Sicherheit, digitalen Resilienz Angreifermodelle und Bedrohungen, Angriffstechniken Schutzziele, Schutz- und Gegenmaßnahmen zur Sicherung von Daten, IT-Systemen und Organisationen Grundlagen der angewandten Kryptographie und des Risiko- und Krisenmanagements

Literature	Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems Wiley; 2. edition (April 14, 2008) ISBN-13: 978-0470068526 Online verfügbar unter http://www.cl.cam.ac.uk/~rja14/book.html Matt Bishop: Computer Security – Art and Science Addison-Wesley Professional; 1. edition (December 12, 2002) ISBN-13: 978-0201440997 Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C Wiley; 2. edition (November 2, 1995) ISBN-13: 978-0471128458

Teaching format of this course	
Teaching format	**SWS**
Lehrvortrag + Übung	2

Examinations	
Ungraded Course Assessment	No

HAW Kiel
Hochschule für Angewandte Wissenschaften Kiel
Kiel University of Applied Sciences

Course: IT-Recht und Datenschutz

General information	
Course Name	IT-Recht und Datenschutz IT-Law and Data Privacy
Course code	ITRD
Lecturer(s)	Prof. Dr. Stark, Thorsten (thorsten.stark@haw-kiel.de)
Occurrence frequency	Regular
Module occurrence	In der Regel im Wintersemester
Language	Deutsch

Qualification outcome
Areas of Competence: Knowledge and Understanding; Use, application and generation of knowledge; Communication and cooperation; Scientific self-understanding / professionalism.
Die Studierenden verstehen die grundlegenden Aspekte des Managements der Cybersicherheit und der digitalen Resilienz. Sie kennen die Grundkonzepte von Angreifermodellen und verstehen im Ansatz die Funktionsweise verschiedener Angriffstechniken. Sie kennen Grundlagen der Kryptographie, ausgewählte Sicherheitsmechanismen, und Systematik von möglichen Schutzmaßnahmen. Sie verstehen die Notwendigkeit für und die Kernelemente von verschiedenen Ansätzen zur Sicherstellung der betrieblichen Kontinuität im Ereignisfall. Die Studierenden kennen grundsätzlich die von IT-Recht und Datenschutz betroffenen Themenfelder.
Die Studierenden können Ebenen der Cybersicherheit im Kontext von Unternehmen oder Organisationen anwenden, inklusive mathematisch-kryptographischer Grundlagen, technischer Maßnahmen, organisatorischer und strategischer Maßnahmen, Elementen menschlichen Verhaltens sowie rechtlichen Aspekten. Die Studierenden sind in der Lage, eigene Analysen zur Cybersicherheit im betrieblichen Umfeld durchzuführen und die Ergebnisse geeignet zu dokumentieren. Sie besitzen erste Kompetenzen zur Durchführung einer Risikobewertung.
Die Studierenden können Problemstellungen der Cybersicherheit und des IT-Rechts erörtern und diskutieren. Die Studierenden können selbst erarbeitete Inhalte mit Bezug zu Cybersicherheit, digitaler Resilienz und IT-Recht verständlich und überzeugend aufbereiten und präsentieren, sowie inhaltliche Aspekte sachgerecht und fachlich kompetent diskutieren. Sie können kompetent einschätzen, wann rechtliche Fragestellungen das Einbeziehen von Expert*innen erfordert.

Content information	
Content	Grundlagen im IT-Recht inklusive Datenschutz, z.B. Abgrenzung Privatrecht / öffentliches Recht / Strafrecht; Vertragsschluss; EDV-Vertragsrecht, Softwareerstellung, Softwareüberlassung, Softwarewartung und Softwarepflege; Datenschutz; Jugendschutz; Domainrecht, Urheberrecht, Wettbewerbsrecht; Haftung im Offline- und Onlinebereich; Strafrecht; Internationale rechtliche Bezüge

Teaching format of this course	
Teaching format	**SWS**
Lehrvortrag + Übung	2

Examinations	
Ungraded Course Assessment	No