

Modulbezeichnung:	Einführung in Datenschutz und IT-Sicherheit	
Modulnummer: DLBINGEDS	Semester: --	Dauer: Minimaldauer 1 Semester
Modultyp: Pflicht		Regulär angeboten im: WS, SS
Workload: 150 h		ECTS Punkte: 5
Zugangsvoraussetzungen:		Unterrichtssprache: Deutsch
Kurse im Modul: <ul style="list-style-type: none"> Einführung in Datenschutz und IT-Sicherheit (DLBISIC01) 		Workload: Selbststudium: 90 h Selbstüberprüfung: 30 h Tutorien: 30 h
Kurskoordinatoren/Tutoren:: Siehe aktuelle Liste der Tutoren im Learning Management System		Modulverantwortliche(r): Prof. Dr. Ralf Kneuper
Bezüge zu anderen Programmen: <ul style="list-style-type: none"> Bachelor Wirtschaftsinformatik Bachelor Wirtschaftsingenieurswesen Industrie 4.0 		Bezüge zu anderen Modulen im Programm:
Qualifikations- und Lernziele des Moduls: Nach der Teilnahme an diesem Modul haben die Studierenden <ul style="list-style-type: none"> grundlegende Kenntnisse zu Begriffen und Konzepten der IT-Sicherheit und wissen, welche typischen Verfahren und Techniken es in welchen Gebieten gibt. grundlegende Kenntnisse der gesetzlichen Regelungen zum Datenschutz und ihrer Umsetzung. vertiefende Kenntnisse zum IT-Sicherheitsmanagement sowie zu geeigneten Maßnahmen zur Umsetzung. Überblickswissen zu Aktivitäten und Strategien zur IT-Sicherheit in der Software- und Systementwicklung. 		
Lehrinhalt des Moduls:		
<ul style="list-style-type: none"> Grundlagen der IT-Sicherheit <ul style="list-style-type: none"> >Datenschutz >IT-Sicherheitsmanagement >Netzwerk- und Kommunikationssicherheit 		
Lehrmethoden:	Siehe Kursbeschreibung	
Literatur:	Siehe Literaturliste der vorliegenden Kursbeschreibung	

Anteil der Modulnote an der Gesamtabschlussnote des Programms: --	Prüfungszulassungsvoraussetzung:	Abschlussprüfungen:
	Siehe Kursbeschreibung	DLBISIC01 Klausur, 90 Min. (100%)

Kursnummer: DLBISIC01	Kursname: Einführung in Datenschutz und IT-Sicherheit	Gesamtstunden: 150 h ECTS Punkte: 5 ECTS
Kurstyp: Pflicht, Wahlpflicht Zu Details beachte bitte das Curriculum des jeweiligen Studiengangs Kursangebot: Kursdauer: Minimaldauer 1 Semester; ab dem 5. Semester wählbar		Zugangsvoraussetzungen: Siehe Modulbeschreibung
Kurskoordinator(en) / Dozenten / Lektoren: Siehe aktuelle Liste der Tutoren im Learning Management System		Bezüge zu anderen Modulen: Siehe Modulbeschreibung
Beschreibung des Kurses: Die Studierenden lernen wichtige Konzepte aus dem Bereich IT-Sicherheit kennen. Dabei werden grundlegende Begriffe eingeführt und diskutiert, typische Anwendungsfelder und Einsatzgebiete von IT-Sicherheit vorgestellt und typische Verfahren und Techniken beschrieben. Kursziele: Nach der Teilnahme an diesem Kurs haben die Studierenden <ul style="list-style-type: none"> • grundlegende Kenntnisse zu Begriffen und Konzepten der IT-Sicherheit und wissen, in welchen Gebieten es welche typischen Verfahren und Techniken gibt. • grundlegende Kenntnisse der gesetzlichen Regelungen zum Datenschutz und ihrer Umsetzung. • vertiefende Kenntnisse zum IT-Sicherheitsmanagement und geeigneter Maßnahmen zur Umsetzung. • Überblickswissen zu Aktivitäten und Strategien zur IT-Sicherheit in der Software- und Systementwicklung. Lehrmethoden: Die Lehrmaterialien enthalten Skripte, Video-Vorlesungen, Übungen, Podcasts, (Online-) Tutorien und Fallstudien. Sie sind so strukturiert, dass Studierende sie in freier Ortswahl und zeitlich unabhängig bearbeiten können. Inhalte des Kurses: <ol style="list-style-type: none"> 1. Begriffsbestimmungen und Hintergründe <ol style="list-style-type: none"> 1.1 Informationstechnik (IT) für die Unterstützung von privaten Aktivitäten und geschäftlichen Prozessen 1.2 Sicherheit und Schutz als Grundbedürfnisse 1.3 Datenschutz als Persönlichkeitsrecht 1.4 IT-Sicherheit als Qualitätsmerkmal in IT-Verbänden 1.5 Abgrenzung Datenschutz und IT-Sicherheit 2. Grundlagen des Datenschutzes <ol style="list-style-type: none"> 2.1 Prinzipien 2.2 Rechtliche Vorgaben 2.3 Informelle Selbstbestimmung im Alltag 		

3. Grundlagen der IT-Sicherheit

3.1 Paradigmen der IT-Sicherheit

3.2 Modelle der IT-Sicherheit

3.3 Rechtliche Vorgaben der IT-Sicherheit

4. Standards und Normen der IT-Sicherheit

4.1 Grundlegende Standards und Normen

4.2 Spezifische Standards und Normen

5. Erstellung eines Sicherheitskonzeptes auf Basis von IT-Grundschutz

5.1 Strukturanalyse

5.2 Schutzbedarfsfeststellung

5.3 Auswahl und Anpassung von Maßnahmen

5.4 Basis-Sicherheitscheck

5.5 Ergänzende Sicherheitsanalyse

6. Bewährte Schutz- und Sicherheitskonzepte für IT-Geräte

6.1 Schutz vor Diebstahl

6.2 Schutz vor Schadsoftware (Malware)

6.3 Sichere Anmeldeverfahren

6.4 Sichere Speicherung von Daten

6.5 Sichere Vernichtung von Daten

7. Ausgewählte Schutz- und Sicherheitskonzepte für IT-Infrastrukturen

7.1 Objektschutz

7.2 Schutz vor unerlaubter Datenübertragung

7.3 Schutz vor unerwünschtem Datenverkehr

7.4 Schutz durch Notfallplanung

Literatur:

- Eckert, C. (2014): IT-Sicherheit. Konzepte - Verfahren - Protokolle. 9. Auflage, De Gruyter Oldenbourg, München. ISBN-13: 978-3486778489.
- Poguntke, W. (2013): Basiswissen IT-Sicherheit. Das Wichtigste für den Schutz von Systemen & Daten. 3. Auflage, W3I, Dortmund. ISBN-13: 978-3868340419.
- Witt, B. C. (2010): Datenschutz kompakt und verständlich. 2. Auflage, Vieweg+Teubner, Wiesbaden. ISBN-13: 978-3834812254.

Prüfungsleistung:

Klausur, 90 Min.

Zeitaufwand Studierenden (in Std.): 150

Selbststudium (in Std.): 90

Selbstüberprüfung (in Std.): 30

Tutorien (in Std.): 30

Durch die weitere Nutzung der Seite stimmst du der Verwendung von Cookies zu.