Kursnummer:	**Kursname:**	**Gesamtstunden:**
DLBISIC01	Einführung in Datenschutz und IT-Sicherheit	150 h
		ECTS Punkte: 5 ECTS
Kurstyp: Pflicht, Wahlpflicht Zu Details beachte bitte das Curriculum des jeweiligen Studiengangs **Kursangebot:** WS, SS **Course Duration:** 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

- 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:

1. Begriffsbestimmungen und Hintergründe

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-Verbünden

1.5 Abgrenzung Datenschutz und IT-Sicherheit

2. Grundlagen des Datenschutzes

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, W3l, Dortmund. ISBN-13: 978-3868340419.
- Witt, B. C. (2010): Datenschutz kompakt und verständlich. 2. Auflage, Vieweg+Teubner, Wiesbaden. ISBN-13: 978-3834812254.

Prüfungszugangsvoraussetzung:

• Kursabhängig: Begleitende Online-Lernkontrolle (max. 15 Minuten je Lektion, bestanden / nicht bestanden)
• Kursevaluation

Prüfungsleistung:

Klausur, 90 Min.

Zeitaufwand Studierenden (in Std.): 150

Selbststudium (in Std.): 90
Selbstüberprüfung (in Std.): 30
Tutorien (in Std.): 30