Informationss 2020) (deleted Information Secur	Modulnummer:						
Bachelor Pflicht/Wahl Wahlpflicht Wahl Sonderfall		Modulbereich: Pflicht					
Anzahl der SWS	$ \begin{array}{c c c c c c c c c c c c c c c c c c c $		Kreditpunkte: 6	Turnus i. d. R. angeboten alle 2 Semester			
Formale Voraussetzungen: -							
Inhaltliche Voraussetzungen: Informationssicherheit							
Vorgesehenes Semester: ab 1. Semester							
Sprache: Deutsch							
<ul> <li>Ziele: Studierende:</li> <li>haben vertiefte Kenntnisse in der Sicherung komplexer soziotechnischer Systeme</li> <li>können komplexe kryptographische Sicherheitsprotokolle bewerten und in ihrem Einsatzbereich weiterentwickeln</li> <li>verstehen Sicherheit als Prozess mit ihren technischen und nicht-technischen Komponenten</li> <li>kennen wichtige Sicherheitsprozesse, so wie sie heute in ISMS eingesetzt werden, und können diese weiterentwickeln</li> </ul>							
Inhalte: Systeme	e:						
Fortgeschrittene Anwendung von Kryptographie							
<ul> <li>ECC und seine Varianten</li> <li>Lebenszyklus kryptographischer Verfahren; Stand aktueller Verfahren</li> <li>Zero-Knowledge-Protokolle, Zero-Knowledge-Password-Proof</li> <li>Zertifikate, Beweiswerterhaltung/LTANS</li> <li>Composability von Sicherheitsprotokollen</li> <li>Browserbasierte Sicherheitsprotokolle (SAML/Liberty, OpenID, OAuth)</li> <li>Grundlagen manipulationssicherer Systeme (tamperproof systems)</li> </ul>							
Prozesse:							
<ul> <li>Stat</li> <li>Security M</li> <li>Awa</li> <li>Incide</li> <li>Log</li> <li>Risk-Asse</li> <li>Risi</li> <li>Qua</li> <li>Insid</li> <li>Security U</li> <li>Usa</li> </ul>	iko-Wahrnehmung alitative und quantitative Modelle der-Threat-Modelle	SW.					
	ipte, Literatur, Programme usw.):						

Form der Prüfung: In der Regel Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung						
Arbeitsaufwand	Präsenz Übungsbetrieb/Prüfungsvorbereitung Summe	56 124 180	h			
Lehrende: Prof. Dr. C. Bormann	,		Verantwortlich: Prof. Dr. C. Bormann			