MODULE HANDBOOK DESCRIPTION

Module designation	*Information Systems Security*	
Code	*FBD4115*	
Semester(s) in which the module is taught	*7 / fourth year*	
Person responsible for the module	*A.S.Rachman, ST., MT.*	
Language	*Indonesian*	
Relation to curriculum	*Elective for Computer Engineering*	
Teaching methods	*lectures, small group discussion, project & case base method.*	
Workload (incl. contact hours, self-study hours)	Contact minutes every week, each week of the 16 weeks/semester: • Lectures: 3 x 50 minutes • Exercises and Assignments: 3 x 60 minutes • Self-study: 3 x 60 minutes. Total study hours = 8 hours 30 minutes/week.	
Credit points	*2 SKS (~3.2 ECTS)*	
Required and recommended prerequisites for joining the module	-	
Module objectives/intended learning outcomes	*1. Students are able to organize the concepts of vulnerabilities, threats, risks, controls, architecture and information security standards;* *2. Students are able to differentiate cryptographic concepts and technologies, access control and identity security;*	*PLO3 (H)*
	3. Students are able to plan the security of data, application, network, and physical; *4. Students are able to reconstruct incident response and computer forensic concepts;*	*PLO4 (M)*
	5. Students are able to to evaluate security risk management, business continuity, security policies and programs.	*PLO5 (L)*

Content	*1. Pendahuluan keamanan sistem informasi* *2. Vulnerabilities, threat, risk & control* *3. Dasar kriptografi* *4. Kendali akses dan manajemen identitas* *5. Keamanan jaringan* *6. Keamanan host dan keamanan data* *7. Keamanan aplikasi berbasis web* *8. Manajemen keamanan informasi*
Examination forms	- *Case based* - *Project based*
Study and examination requirements	*The final grade in the module is composed of:* *a. Case I assessment: 20%* *b. Case II assessment: 20%* *c. Project based: 60%* *Students must have a final grade of 65% or higher to pass*
Reading list	*1. Andy Taylor, David Alexander, Amanda Finch, David Sutton, 2018, Information Security Management Principles, BCS, The Chartered Institute for IT;* *2. Handbook for Computer Security Incident Response Teams http://www.cert.org/archive/pdf/csirt-handbook.pdf* *3. E.Wheeler,2011,"Security Risk Management: Building an Information Security Risk Management Program from the Ground Up", Syngress* *4. Gurjar, L.R., 2009, Cyber securities and Cyber Terrorism, Vardhaman Mahaveer Open* *5. HM Government, Cyber Essentials Scheme Requirements for basic technical protection from cyber attacks, 2014 Online: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf* *6. Handbook of Security, Cryptography and Digital Signature by P. Ramchandaran & S.M. Bhaskar (Viva Book Pvt. Ltd.)* *7. Sheward, mike, Hands-on Incident Response and Digital Forensics, Imprint: BCS, The Chartered Institute for IT, 2018*