MODULE HANDBOOK DESCRIPTION

Module designation	Computer Network Security	
Code	FBD0005	
Semester(s) in which the module is taught	Third Year	
Person responsible for the module	L. Ahmad Syamsul Irfn Akbar, ST.,M.Eng	
Language	Indonesian	
Relation to curriculum	Free elective for Computer Engineering	
Teaching methods	lectures, cooperative Learning	
Workload (incl. contact hours, self-study hours)	Contact minutes every week, each week of the 16 weeks/semester: • Lectures: 2 x 50 minutes • Exercises and Assignments: 2 x 60 minutes • Self-study: 2 x 60 minutes. Total study hours = 5 hours 40 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 analyze network security issues, solve those problems, and implement the appropriate and effective solutions. In addition, students are also expected to evaluate existing network security and develop better security systems. To achieve this PLO, students will be equipped with knowledge and skills in applying network security concepts, such as data encryption, threat identification, access management, and so on. Students are also expected to keep up with the latest developments in network security technology and be able to apply it in complex business environments.	PLO3

	2. Students are able to build, design, and plan effective and reliable computer network security systems. They are expected to apply network security concepts in complex business environments, including the latest technologies, and evaluate existing security systems. To achieve this PLO, students will learn and master the basic concepts of network security, cryptography techniques, access management, firewall and IDPS technologies, as well as VPN technology.	PLO 4
	3. Students will be able to relate and analyze the network security concepts learned in this course with the latest technology developments and security challenges. In addition, students can scrutinize and evaluate existing network security policies and recommend necessary improvements. In achieving this PLO, students will continue to enhance their lifelong learning skills and develop the ability to renew knowledge and keep up with the latest developments in the field of network security.	PLO9
Content	- Introduction to network security - Types of threats and attacks - Network topologies and security issues - Firewall technologies and configurations - Intrusion Detection and Prevention Systems (IDPS) - Virtual Private Network (VPN) and secure remote access - Authentication and Access Control Mechanisms - Public Key Infrastructure (PKI) - Cryptography and Encryption Techniques - Wireless Network Security - Incident Response and Disaster Recovery Planning - Legal and Ethical Issues in Network Security.	
	- Complete the group task - Midterm and final test	
Study and examination requirements	The final grade in the module is composed of: a. Attendance: 10% b. Case assessment: 4 x 15% = 60% c. Midterm assessment: 15% d. Final assessment: 15% Students must have a final grade of 65% or higher to pass	

Reading list	1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson. 2. Bishop, M. (2018). Computer Security: Art and Science (2nd ed.). Addison-Wesley.