Module Description

Module name	Digital Security
Module level, if applicable	Bachelor of Informatics
Code, if applicable	21D12121503
Subtitle, if applicable	-
Course, if applicable	-
Semester(s) in which the module is taught	4th
Person responsible for the module	Dr. Eng. Ady Wahyudi Paundu
Lecturer	1. Dr. Eng. Ady Wahyudi Paundu 2. Iqra Aswad, S.T., M.T.
Language	Indonesian Language [Bahasa Indonesia]
Relation to Curriculum	This course is a compulsory course and is offered in the 4th semester.
Type of teaching, contact hours	Teaching methods: [group discussion], [case study], [collaborative learning], [problem-based learning]. Teaching forms: [lecture], [tutorial], [practicum]. CH : 08.00 - 16.00
Workload	For this course, students are required to meet a minimum of 136.00 hours in one semester, which consist of: - 40.00 hours for lecture, - 48.00 hours for structured assignments, - 48.00 hours for private study
Credit points	3 credit points (equivalent with 5.1 ECTS)
Requirements according to the	Students have participated in at least 80% of the learning activities (Academic Regulations, Chapter VII)

examination regulations	
Recommended prerequisites	-
Module objectives/intended learning outcomes	After completing the course, Students are able: **Intended Learning Outcomes (ILO):** **ILO 1 :** Have the knowledge of fundamental in Computing Science that includes basic theory and concepts of computer science, Mathematics and Statistics, Programming Algorithm, Software Engineering, Information Management and Digital Resilience, also the advance topics of either Artificial Intelligence, Data Science, Computer Network, Cloud Computing or Internet of Things. **ILO 3 :** Apply the knowledge of computing and other related disciplines to analyse and identify solutions for any computing-based problem **Course Learning Objective (CLO):** After taking the Internet Security Course for one semester, students are able to understand the basic principles of internet security and various aspects in it including design, monitoring, detection, maintenance, management, and restoration to analyze and deliver solutions. **Sub CLO :** ILO 1 ⇒ CLO 1: Students understand the basic principles of internet security and the importance of humanware (human aspect as a user) to maintaining internet security. ILO 3 ⇒ CLO 2: Students understand working principles of several main functions of internet security such as authentication, authorization, cryptography, intrusion detection, and forensic operation. Students also know the principles of security at various computing layers, including the application layer, database, operating system, and computer network and are able to perform simple security operations at each of these layers.

<table>
<tr><td></td><td>ILO 1 ⇒ CLO 3: Students understand the principles of non-technical aspects of the internet security system such as regulation aspect, ethics, privacy, management, policy and governance.
ILO 1 ⇒ CLO 4: Students understand the latest issues regarding advances in internet security technology and the latest security threats.</td></tr>
<tr><td>Content</td><td>Students will learn about :
1. Cybersecurity functions
2. The basic principle of cybersecurity design
3. Authentication and Authorization system
4. Cryptography and cryptanalysis method
5. Security mechanism of application and database, operating system and network.
6. Intrusion detection mechanism
7. Digital Forensic concept.
8. Social Engineering
9. Computer security operation, maintenance, regulation and policy
10. Privacy and ethics issues
11. Cybersecurity governance
12. Common tools in internet security operation
13. Advanced Persistent Threat
14. Latest digital security issues</td></tr>
<tr><td>Forms of Assessment</td><td>Assessment techniques: [observation], [performance], [written test].

Assessment forms: [midterm exam], [assignment].

<table><tr><td>CLO 1</td><td colspan="2">CLO 2</td><td>CLO 3</td><td>CLO 4</td></tr><tr><td>Assign 1</td><td>Assign 2</td><td>Exam1</td><td>Exam2</td><td>Assign3</td></tr><tr><td>20%</td><td>30%</td><td>20%</td><td>10%</td><td>20%</td></tr></table></td></tr>
<tr><td>Study and examination requirements and forms of examination</td><td>Study and examination requirements:
- Students must attend 15 minutes before the class starts.
- Students must switch off all electronic devices.
- Students must inform the lecturer if they will not attend the class due to sickness, etc.</td></tr>
</table>

	- Students must submit all class assignments before the deadline. - Students must attend the exam to get the final grade. **Form of examination:** Written exam
Media employed	Video conference, slide presentation, Learning Management System (LMS)
Reading list	**Main :** William Stallings and Lawrie Brown, 2019, Computer Security: Principles and Practice, 4th ed, Pearson Education Inc. ISBN 978-9-35-343886-9