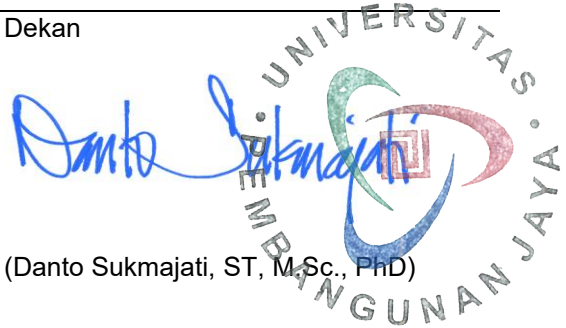
RENCANA PEMBELAJARAN SEMESTER (RPS)
PROGRAM STUDI SISTEM INFORMASI
FAKULTAS TEKNOLOGI DAN DESAIN

SPT-I/03/BP/P0B-01/F-02

Issue/Revisi : A0

Mata Kuliah	**Keamanan Jaringan Sistem Informasi (*Information System Network Security*)**	Tanggal	:1 Agustus 2024
Kode MK	: SIF303	Rumpun MK	: MKWP
Bobot (sks)	T (Teori) : 2 P (Praktik/Praktikum) : 1	Semester	: 5
Dosen Pengembang RPS,  (Johannes Hamonangan Siregar,PhD.)	Koordinator Keilmuan  (Johannes Hamonangan Siregar, PhD)	Kepala Program Studi,  (Chaerul Anwar, S.Kom, MTI)	Dekan  (Danto Sukmajati, ST, M.Sc., PhD)

RENCANA PEMBELAJARAN SEMESTER		
Capaian Pembelajaran (CP)	**CPL – PRODI yang dibebankan pada MK**	
	23-SIF-CPL-06	Menguasai metode pengelolaan dan keamanan sesuai dengan kode etik untuk menjamin kerahasiaan, integritas, ketersediaan, serta keberlanjutan sistem informasi
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	23-SIF-CPMK-061	Menguasasi metode pengelolaan keamanan
	23-SIF-CPMK-062	Menguasai prinsip kode etik dalam keamanan sistem
	23-SIF-CPMK-063	Menguasai prinsip kerahasiaan, integritas, dan ketersediaan sistem informasi
	23-SIF-CPMK-064	Mampu melakukan pengamanan yang menjamin ketersediaan sistem informasi
	Kemampuan Akhir Tiap Tahap Belajar (Sub-CPMK)	
	23-SIF-SCPMK-0611	Mampu menjelaskan konsep keamanan teknologi informasi pada organisasi.

RENCANA PEMBELAJARAN SEMESTER

	23-SIF-SCPMK-0621	Mampu menjelaskan konsep dasar keamanan informasi, termasuk integritas, kerahasiaan, ketersediaan, dan autentikasi.
	23-SIF-SCPMK-0622	Mampu mengidentifikasi berbagai ancaman serta menganalisis kerentanan pada sistem informasi dan jaringan, sehingga mengerti tentang celah keamanan dan bagaimana kerentanan ini dapat dieksploitasi oleh penyerang.
	23-SIF-SCPMK-0623	Mampu menjelaskan prinsip dasar kriptografi dan mengerti bagaimana teknik yang dapat digunakan untuk melindungi data dan dari akses yang tidak sah.
	23-SIF-SCPMK-0631	Mampu mengidentifikasi dan mengatasi potensi kerentanan pada perangkat lunak dan aplikasi yang digunakan dalam lingkungan organisasi.
	23-SIF-SCPMK-0632	Mampu merancang dan menerapkan kebijakan keamanan yang sesuai dengan kebutuhan dan lingkungan organisasi.
	23-SIF-SCPMK-0633	Mampu memahami Etika dan Hukum memahami isu-isu etika dan hukum yang terkait dengan keamanan informasi, termasuk hak cipta, privasi, dan tanggung jawab dalam penggunaan teknologi informasi.
	23-SIF-SCPMK-0634	Mampu memahami bagaimana mengidentifikasi, menanggapi, dan mengatasi insiden keamanan.
	23-SIF-SCPMK-0641	Mampu bekerja dalam tim keamanan informasi dan berkontribusi dalam menghadapi tantangan keamanan yang kompleks.
	23-SIF-SCPMK-0642	Mampu memperbaharui pengetahuan tentang perkembangan terbaru dalam bidang keamanan jaringan dan sistem informasi.
	Korelasi CPMK terhadap Sub-CPMK	

	23-SIF-SCPMK-0611	23-SIF-SCPMK-0621	23-SIF-SCPMK-0622	23-SIF-SCPMK-0623	23-SIF-SCPMK-0631	23-SIF-SCPMK-0632	23-SIF-SCPMK-0633	23-SIF-SCPMK-0634	23-SIF-SCPMK-0641	23-SIF-SCPMK-0642
23-SIF-CPMK-061	√									

RENCANA PEMBELAJARAN SEMESTER

	23-SIF-CPMK-062		√	√	√						
	23-SIF-CPMK-063					√	√	√	√		
	23-SIF-CPMK-064									√	√

Kode CPL	Kode CPMK	Kode Sub CPMK	Indikator	Metode Penilaian	Bobot
23-SIF-CPL-06	23-SIF-CPMK-061	23-SIF-SCPMK-0611	Mampu menjelaskan konsep keamanan teknologi informasi pada organisasi.	Kuis (5%)	5%
	23-SIF-CPMK-062	23-SIF-SCPMK-0621	Mampu menjelaskan konsep dasar keamanan informasi, termasuk integritas, kerahasiaan, ketersediaan, dan autentikasi.	Kuis (5%) , Tugas (10%)	15%
		23-SIF-SCPMK-0622	Mampu mengidentifikasi berbagai ancaman serta menganalisis kerentanan pada sistem informasi dan jaringan, sehingga mengerti tentang celah keamanan dan bagaimana kerentanan ini dapat dieksploitasi oleh penyerang.		
		23-SIF-SCPMK-0623	Mampu menjelaskan prinsip dasar kriptografi dan mengerti bagaimana teknik yang dapat digunakan untuk melindungi data dan dari akses yang tidak sah.		
	23-SIF-CPMK-063	23-SIF-SCPMK-0631	Mampu mengidentifikasi dan mengatasi potensi kerentanan pada perangkat lunak dan aplikasi yang digunakan dalam lingkungan organisasi.	Kuis (5%) Tugas (15%), UTS (20%)	40%

RENCANA PEMBELAJARAN SEMESTER

		23-SIF-SCPMK-0632	Mampu merancang dan menerapkan kebijakan keamanan yang sesuai dengan kebutuhan dan lingkungan organisasi.		
		23-SIF-SCPMK-0633	Mampu memahami Etika dan Hukum memahami isu-isu etika dan hukum yang terkait dengan keamanan informasi, termasuk hak cipta, privasi, dan tanggung jawab dalam penggunaan teknologi informasi.		
		23-SIF-SCPMK-0634	Mampu memahami bagaimana mengidentifikasi, menanggapi, dan mengatasi insiden keamanan.		
	23-SIF-CPMK-064	23-SIF-SCPMK-0641	Mampu bekerja dalam tim keamanan informasi dan berkontribusi dalam menghadapi tantangan keamanan yang kompleks.	Tugas (10%), Proyek Kelompok (30%)	40%
		23-SIF-SCPMK-0642	Mampu memperbaharui pengetahuan tentang perkembangan terbaru dalam bidang keamanan jaringan dan sistem informasi		

Deskripsi Singkat MK	Mata kuliah memberikan pengalaman belajar kepada mahasiswa tentang model dan bentuk berupa teknologi jaringan korporasi, pengendalian keamanan jaringan komunikasi data, keamanan data atau informasi, dan secure code untuk sebuah sistem informasi. Pengorganisasian terhadap monitoring sistem informasi (paket data), keamanan teknologi informasi dan komunikasi pada organisasi, perencanaan dan monitoring sistem informasi. Melalui mata kuliah ini, mahasiswa diharapkan mampu memahami, merancang, dan mengaplikasikan daya guna teknologi informasi dengan konsep infrastruktur teknologi informasi pada suatu korporasi.
Bahan Kajian : Materi Pembelajaran/Pokok Bahasan	1 Konsep dasar keamanan informasi dan prinsip CIA (Confidentiality, Integrity, Availability) 2 Ancaman dan kerentanan pada sistem informasi dan jaringan 3 Dasar-dasar kriptografi: enkripsi simetris dan asimetris, algoritma kriptografi populer

<table>
<tr><th colspan="3">RENCANA PEMBELAJARAN SEMESTER</th></tr>
<tr><td></td><td colspan="2">4 Kerentanan perangkat lunak dan aplikasi, OWASP Top 10, teknik pengamanan perangkat lunak
5 Kebijakan dan prosedur keamanan informasi dalam organisasi: ISO/IEC 27001, NIST
6 Etika dan hukum dalam keamanan informasi: privasi, hak cipta, UU ITE, GDPR
7 Penanganan insiden keamanan informasi: identifikasi, respons, pemulihan, CSIRT
8 Kerja tim keamanan informasi: struktur tim, kolaborasi dalam penanganan ancaman
9 Perkembangan dan tren terbaru dalam keamanan jaringan dan sistem informasi (misalnya Zero Trust, Threat Intelligence, keamanan IoT, AI Security)</td></tr>
<tr><td rowspan="4">Pustaka</td><td colspan="2">Utama</td></tr>
<tr><td colspan="2">Michael E. Whitman and Herbert J. Mattord, 2022, Principles of Information Security, 7th Edition, Cengage Learning, Inc</td></tr>
<tr><td colspan="2">Pendukung</td></tr>
<tr><td colspan="2">Michael Collins, 2015, Network Security Through Data Analysis, Building Situational Awareness, O’Reilly
Stallings, William. 2020, Cryptography and network security : principles and practice. Pearson</td></tr>
<tr><td rowspan="2">, Media Pembelajaran</td><td>Perangkat Lunak:</td><td>Perangkat Keras:</td></tr>
<tr><td>Cisco Packet Tracer</td><td>Komputer / Laptop</td></tr>
<tr><td>Dosen Pengampu</td><td colspan="2">Johannes Hamonangan Siregar, PhD</td></tr>
<tr><td>Mata Kuliah Prasyarat</td><td colspan="2">(jika ada)</td></tr>
<tr><td>Indikator, Kriteria, dan Bobot Penilaian</td><td colspan="2">
<table>
<tr><th>Komponen Penilaian</th><th>Bobot</th></tr>
<tr><td>Ujian Tengah Semester</td><td>20%</td></tr>
<tr><td>Ujian Akhir Semester</td><td>-</td></tr>
<tr><td>Presensi/Kehadiran</td><td>-</td></tr>
<tr><td>Tugas</td><td>35%</td></tr>
<tr><td>Project</td><td>30%</td></tr>
<tr><td>Kuis</td><td>15%</td></tr>
<tr><td>Diskusi Kelas</td><td>-</td></tr>
</table>
</td></tr>
</table>

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
1	23-SIF-SCPMK-0611 Mampu menjelaskan konsep keamanan teknologi informasi pada organisasi	Mahasiswa dapat menjelaskan kebijakan dan prosedur keamanan informasi dalam organisasi.	Kriteria penilaian: Penguasaan dan Pemahaman. Bentuk penilaian: -Kuis	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		- Ancaman dan kerentanan (threats & vulnerabilities) - Standar keamanan informasi	5
2	23-SIF-SCPMK-0621 Mampu menjelaskan konsep dasar keamanan informasi, termasuk integritas, kerahasiaan, ketersediaan, dan autentikasi..	Mahasiswa dapat menjelaskan prinsip dasar keamanan informasi (Confidentiality, Integrity, Availability – CIA)	Kriteria penilaian: Penguasaan dan Pemahaman. Bentuk penilaian: Tugas -	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		- Prinsip dasar keamanan informasi (CIA Triad) - Kebijakan dan prosedur keamanan	10
3	23-SIF-SCPMK-0622 Mampu mengidentifikasi berbagai ancaman serta menganalisis kerentanan pada sistem informasi dan jaringan, sehingga mengerti tentang celah keamanan dan bagaimana kerentanan ini dapat dieksploitasi oleh penyerang.	Mahasiswa mampu menjelaskan konsep vulnerability, exploit, dan threat modeling	Kriteria penilaian: Penguasaan dan Pemahaman. Bentuk penilaian: Kuis	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		- Klasifikasi ancaman dan serangan - Kerentanan sistem dan jaringan - Tools pemindaian dan analisis - Threat modeling dan risk assessment - Studi kasus eksploitasi kerentanan	5
4	23-SIF-SCPMK-0623 Mampu menjelaskan prinsip dasar kriptografi dan mengerti bagaimana teknik	Mahasiswa mampu menjelaskan konsep dasar kriptografi (plaintext, ciphertext, key, algoritma)	Kriteria penilaian: Penguasaan dan Pemahaman.		Bentuk pembelajaran: Asinkronus Online	Konsep dasar kriptografi - Enkripsi simetris vs. asimetris	10

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
	yang dapat digunakan untuk melindungi data dan dari akses yang tidak sah.		Bentuk penilaian: Tugas		Metode pembelajaran: Partisipasi (diskusi Online) melalui Forum di Collabor Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'	- Algoritma kriptografi populer	
5		Mahasiswa mampu memberikan contoh penerapan kriptografi dalam organisasi	Kriteria penilaian: Penguasaan dan Pemahaman. Bentuk penilaian: -	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		- Public Key Infrastructure (PKI) - Aplikasi kriptografi dalam dunia nyata	
6	23-SIF-SCPMK-0631 Mampu mengidentifikasi dan mengatasi potensi kerentanan pada perangkat lunak dan aplikasi yang digunakan dalam lingkungan organisasi.	Mahasiswa mampu menjelaskan jenis jenis kerentanan umum pada perangkat lunak	Kriteria penilaian: Penguasaan dan Pemahaman. Bentuk penilaian:	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		- Jenis kerentanan perangkat lunak dan aplikasi - Tools scanning dan vulnerability assessment	
7		Melakukan analisis terhadap studi kasus insiden keamanan akibat kerentanan aplikasi	Kriteria penilaian: Penguasaan dan Pemahaman. Bentuk penilaian:	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Estimasi waktu: TM = 2 x 50' BM = 2 x 60'		- Konsep secure coding dan update sistem - Studi kasus kerentanan nyata dan respons organisasi	

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
				BS = 2 x 60’			
8	**Evaluasi Tengah Semester : Melakukan validasi hasil penilaian, evaluasi dan perbaikan proses pembelajaran berikutnya**						
9	23-SIF-SCPMK-0632 Mampu merancang dan menerapkan kebijakan keamanan yang sesuai dengan kebutuhan dan lingkungan organisasi.	Menjelaskan komponen utama dalam kebijakan keamanan informasi	Penguasaan dan Pemahaman. Bentuk penilaian: Kuis	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Estimasi waktu: TM = 2 x 50’ BM = 2 x 60’ BS = 2 x 60’		- Struktur dan komponen kebijakan keamanan - Analisis kebutuhan dan risiko organisasi - Proses perumusan dan penerapan kebijakan - Studi kasus kebijakan keamanan di perusahaan nyata - Evaluasi dan perbaikan kebijakan keamanan	5
10	23-SIF-SCPMK-0633 Mampu memahami Etika dan Hukum memahami isu-isu etika dan hukum yang terkait dengan keamanan informasi, termasuk hak cipta, privasi, dan tanggung jawab dalam penggunaan teknologi informasi.	Mengidentifikasi bentuk pelanggaran hukum terkait keamanan informasi (misal: pelanggaran privasi, penyalahgunaan data, pelanggaran hak cipta)	Penguasaan dan Pemahaman. Bentuk penilaian: Tugas	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Estimasi waktu: TM = 2 x 50’ BM = 2 x 60’ BS = 2 x 60’		- Etika dalam keamanan informasi - Hak cipta, privasi, dan tanggung jawab digital - Studi kasus pelanggaran etika dan hukum dalam TI	15
11	23-SIF-SCPMK-0634 Mampu memahami bagaimana mengidentifikasi, menanggapi, dan mengatasi insiden keamanan.	Mengidentifikasi jenis-jenis insiden keamanan (misal: DDoS, malware, data breach)	Penguasaan dan Pemahaman. Bentuk penilaian: Tugas	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah		- Konsep insiden keamanan informasi - Siklus penanganan insiden (Incident	

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
				Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		Response Lifecycle) - CSIRT dan peranannya - Tools untuk identifikasi dan pelaporan insiden - Dokumentasi dan evaluasi insiden	
12	23-SIF-SCPMK-0641 Mampu bekerja dalam tim keamanan informasi dan berkontribusi dalam menghadapi tantangan keamanan yang kompleks.	Mahasiswa mampu menjelaskan peran dan struktur tim keamanan informasi	Penguasaan dan Pemahaman. Bentuk penilaian: Tugas-		Bentuk pembelajaran: Asinkronus Online Metode pembelajaran: Partisipasi (diskusi Online) melalui Forum di Collabor Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'	- Struktur dan fungsi tim keamanan informasi - Simulasi Blue Team vs Red Team	10
13		Mahasiswa berpartisipasi aktif dalam simulasi kerja tim untuk menyelesaikan permasalahan keamanan		Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		- Teknik kolaborasi dalam respons insiden - Studi kasus kerja tim dalam menghadapi ancaman dunia nyata - Evaluasi kontribusi tim dalam proyek keamanan	
14	23-SIF-SCPMK-0642 Mampu memperbaharui pengetahuan tentang perkembangan terbaru dalam bidang keamanan jaringan dan sistem informasi	Mahasiswa mampu menjelaskan tren dan ancaman terkini di bidang keamanan jaringan	Penguasaan dan Pemahaman. Bentuk penilaian: Tugas Proyek	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah		- Tren ancaman keamanan terbaru - Teknologi keamanan mutakhir	30

Minggu ke-	Sub CP-MK (Kemampuan Akhir yang Diharapkan)	Penilaian		Bentuk Pembelajaran: Metode Pembelajaran; Penugasan Mahasiswa (Estimasi Waktu)		Materi Pembelajaran (Pustaka)	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk Penilaian				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
				Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		- Sumber informasi terpercaya di bidang keamanan TI (blog, jurnal, vendor reports)	
15		Mahasiswa mampu menyampaikan ringkasan atau ulasan perkembangan terbaru secara lisan atau tulisan	Penguasaan dan Pemahaman. Bentuk penilaian: -	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		- Analisis artikel atau berita keamanan aktual - Critical thinking dalam membaca perkembangan TI	
16	**Evaluasi Akhir Semester: Melakukan validasi penilaian akhir dan menentukan kelulusan mahasiswa**						