

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

SPT-I/XXX/XXX

Issue/Revisi : A0

Mata Kuliah	: Introduction to Cybersecurity	Tanggal	: 03 Februari 2025
Kode MK	: INF108	Rumpun MK	: MKWP
Bobot (sks)	T (Teori) : 2 P (Praktik/Praktikum) : 1	Semester	: 2
Dosen Pengembang RPS,	Koordinator Keilmuan,	Kepala Program Studi,	Dekan
 Hendi Hermawan, S.T., M.T.I.	 Mohammad Nasucha, S.T., M.Sc., Ph.D.	 Dr. Ida Nurhaida, S.T., M.T.	 Danto Sukmajati, S.T., M.Sc., Ph.D

RENCANA PEMBELAJARAN SEMESTER		
Capaian Pembelajaran (CP)	CPL – PRODI yang dibebankan pada MK	
	23-INF-CPL-03	Memiliki pengetahuan yang memadai terkait dengan cara kerja sistem komputer dan mampu merancang, mengembangkan dan menerapkan/menggunakan berbagai algoritma/metode untuk memecahkan masalah.
	23-INF-CPL-04	Kemampuan menganalisis persoalan computing yang kompleks serta menerapkan prinsip-prinsip computing dan disiplin ilmu relevan lainnya untuk mengidentifikasi solusi, dengan mempertimbangkan wawasan perkembangan ilmu transdisiplin.
	23-INF-CPL-06	Mampu menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora yang sesuai dengan bidang keahliannya.
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	23-INF-CPMK-031	Mampu memahami cara kerja sistem komputer.
	23-INF-CPMK-032	Mampu merancang, mengembangkan dan menerapkan/menggunakan berbagai algoritma/metode untuk memecahkan masalah.

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

SPT-I/XXX/XXX

Issue/Revisi : A0

RENCANA PEMBELAJARAN SEMESTER								
	23-INF-CPMK-041	Mampu menganalisis persoalan computing yang kompleks.						
	23-INF-CPMK-042	Mampu menerapkan prinsip-prinsip computing dan disiplin ilmu relevan lainnya untuk mengidentifikasi solusi, dengan mempertimbangkan wawasan perkembangan ilmu transdisiplin.						
	23-INF-CPMK-061	Mampu menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi ilmu pengetahuan dan teknologi.						
	Kemampuan Akhir Tiap Tahap Belajar (Sub-CPMK)							
	23-INF-SCPMK-0311	Kemampuan memahami cara kerja sistem komputer.						
	23-INF-SCPMK-0321	Kemampuan merancang algoritma untuk memecahkan masalah.						
	23-INF-SCPMK-0322	Kemampuan mengembangkan algoritma untuk memecahkan masalah.						
	23-INF-SCPMK-0323	Kemampuan menerapkan berbagai algoritma untuk memecahkan masalah.						
	23-INF-SCPMK-0411	Kemampuan menganalisis persoalan computing yang kompleks.						
	23-INF-SCPMK-0421	Kemampuan menerapkan prinsip-prinsip computing dan disiplin ilmu relevan lainnya untuk mengidentifikasi solusi, dengan mempertimbangkan wawasan perkembangan ilmu transdisiplin.						
	23-INF-SCPMK-0611	Kemampuan menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi ilmu pengetahuan dan teknologi.						
	Korelasi CPMK terhadap Sub-CPMK							
		23-INF-SCPMK-0311	23-INF-SCPMK-0321	23-INF-SCPMK-0322	23-INF-SCPMK-0323	23-INF-SCPMK-0411	23-INF-SCPMK-0421	23-INF-SCPMK-0611
	23-INF-CPMK-031	v						
	23-INF-CPMK-032		v	v	v			
23-INF-CPMK-041					v			
23-INF-CPMK-042						v		
23-INF-CPMK-061							v	

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

SPT-I/XXX/XXX

Issue/Revisi : A0

RENCANA PEMBELAJARAN SEMESTER					
Kode CPL	Kode CPMK	Kode Sub CPMK	Indikator	Metode Penilaian	Bobot
23-INF-CPL-03	23-INF-CPMK-031	23-INF-SCPMK-0311	Kemampuan memahami cara kerja sistem komputer.	Forum	10%
	23-INF-CPMK-032	23-INF-SCPMK-0321	Kemampuan merancang algoritma untuk memecahkan masalah.		
		23-INF-SCPMK-0322	Kemampuan mengembangkan algoritma untuk memecahkan masalah.	Tugas	20%
		23-INF-SCPMK-0323	Kemampuan menerapkan berbagai algoritma untuk memecahkan masalah.		
23-INF-CPL-04	23-INF-CPMK-041	23-INF-SCPMK-0411	Kemampuan menganalisis persoalan computing yang kompleks.	UTS	30%
	23-INF-CPMK-042	23-INF-SCPMK-0421	Kemampuan menerapkan prinsip-prinsip computing dan disiplin ilmu relevan lainnya untuk mengidentifikasi solusi, dengan mempertimbangkan wawasan perkembangan ilmu transdisiplin.		
23-INF-CPL-06	23-INF-CPMK-061	23-INF-SCPMK-0611	Kemampuan menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi ilmu pengetahuan dan teknologi.	UAS	30%
Deskripsi Singkat MK		Mata kuliah ini bertujuan untuk memberikan pemahaman kepada mahasiswa tentang mendesain dan membuat aplikasi web, cara berpikir secara prosedural atau berorientasi objek untuk memecahkan persoalan dalam membangun sebuah aplikasi web. Dalam mata kuliah ini juga akan dibangun sebuah proyek aplikasi web. Materi yang diberikan meliputi web database beserta integrasinya, pengenalan konsep Object Oriented dalam aplikasi web, pengenalan PHP Data Object, pengenalan konsep Model View Controller (MVC), dan penyelesaian proyek aplikasi web. Setelah mengikuti perkuliahan ini, mahasiswa diharapkan dapat memahami bagaimana cara mendesain dan membuat sebuah aplikasi web.			
Bahan Kajian : Materi Pembelajaran/Pokok Bahasan		1. Cybersecurity Threats, Vulnerabilities, and Attacks 2. Securing Networks 3. Attacking the Foundation 4. Attacking What We Do 5. Wireless Network Communication Devices 6. Network Security Infrastructure 7. Windows Security & Linux Overview 8. System and Endpoint Protection 9. Cybersecurity Principles, Practices, and Processes 10. System and Network Defense 11. Firewall Technologies 12. Cloud Security			

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

SPT-I/XXX/XXX

Issue/Revisi : A0

RENCANA PEMBELAJARAN SEMESTER							
	13. Cryptography 14. Technologies and Protocols						
Pustaka	Utama						
	Modul Course Cybersecurity essential 3.0 Cisco Academy						
	Pendukung						
Media Pembelajaran	Perangkat Lunak:		Perangkat Keras:				
	LMS Collabor Power point Packet Tracer		Komputer/Laptop				
Dosen Pengampu	Hendi Hermawan						
Mata Kuliah Prasyarat	-						
Indikator, Kriteria, dan Bobot Penilaian	SCPMK	Penilaian dan Bobot				Total Bobot Penilaian	
		Forum	Forum	Tugas	UTS		UAS
		Partisipasi (Kemampuan literasi)	Partisipasi (Kemampuan literasi)	Partisipasi (Kemampuan Praktikum)	Observasi (Studi Kasus)		Observasi (Studi Kasus)
	23-INF-SCPMK-0311	10%					10%
	23-INF-SCPMK-0321		10%				10%
	23-INF-SCPMK-0322			10%			10%
	23-INF-SCPMK-0323			10%			10%

RENCANA PEMBELAJARAN SEMESTER							
	23-INF-SCPMK-0411				30%		20%
	23-INF-SCPMK-0421					10%	10%
	23-INF-SCPMK-0611					20%	20%
	Total per penilaian	10%	10%	20%	30%	30%	100%

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	Luring (5)	Daring (6)		
(1)	(2)	(3)	(4)			(7)	
1	Kemampuan memahami cara kerja sistem komputer. (23-INF-SCPMK-0311) Kemampuan yang diharapkan: Mampu memahami konsep keamanan siber dan infrastruktur sistem komputer.	Kemampuan memahami konsep keamanan siber dan infrastruktur sistem komputer.	Kriteria: Pemahaman Bentuk Penilaian: • Forum	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Partisipasi (Keaktifan) Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		Cybersecurity Threats, Vulnerabilities, and Attacks	1.43%
2	Kemampuan merancang algoritma untuk memecahkan masalah. (23-INF-SCPMK-0321)	Kemampuan memahami jenis serangan dan teknik	Kriteria: Penguasaan Bentuk Penilaian: • Forum	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran:		Securing Networks	1.43%

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

SPT-I/XXX/XXX

Issue/Revisi : A0

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)	
	Kemampuan yang diharapkan: Mampu memahami serangan pada sistem komputer dan mitigasi ancaman.	mitigasi terhadap ancaman siber.		Ceramah Partisipasi (Keaktifan) <u>Estimasi waktu:</u> TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'			
3	Kemampuan mengembangkan algoritma untuk memecahkan masalah. (23-INF-SCPMK-0322) Kemampuan yang diharapkan: Mampu menganalisis serangan berbasis jaringan dan keamanan jaringan.	Kemampuan dalam pemahaman tentang serangan berbasis jaringan dan keamanan jaringan.	Kriteria: Penguasaan Bentuk Penilaian: • Tugas	<u>Bentuk pembelajaran:</u> Tatap muka di kelas <u>Metode pembelajaran:</u> Ceramah Partisipasi (Keaktifan) <u>Estimasi waktu:</u> TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		Attacking the Foundation	2.86%
4	Kemampuan menerapkan berbagai algoritma untuk memecahkan masalah (23-INF-SCPMK-0323) Kemampuan yang diharapkan: Mampu mengimplementasikan pertahanan jaringan dan enkripsi data.	Kemampuan dalam Pemahaman tentang teknik pertahanan jaringan dan enkripsi data.	Kriteria: Penguasaan Bentuk Penilaian: Tugas	<u>Bentuk pembelajaran:</u> Tatap muka di kelas <u>Metode pembelajaran:</u> Ceramah Partisipasi (Keaktifan) <u>Estimasi waktu:</u> TM = 2 x 50' BM = 2 x 60'		Attacking What We Do	2.86%

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'			
5	Kemampuan menganalisis persoalan computing yang kompleks (23-INF-SCPMK-0411) Kemampuan yang diharapkan: Mampu memahami sistem keamanan endpoint dan mitigasi malware.	Kemampuan dalam pemahaman tentang sistem keamanan endpoint dan strategi mitigasi malware.	Kriteria: Penguasaan Bentuk Penilaian: • Tugas	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Partisipasi (Keaktifan) Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		Wireless Network Communication Devices	2.86%
6	Kemampuan memahami cara kerja sistem komputer. (23-INF-SCPMK-0311) Kemampuan yang diharapkan: Mampu menjelaskan strategi pertahanan dalam keamanan siber.	Kemampuan dalam Pemahaman tentang strategi pertahanan dalam keamanan siber.	Kriteria: Penguasaan Bentuk Penilaian: Forum	Bentuk pembelajaran: Tatap muka di kelas Metode pembelajaran: Ceramah Partisipasi (Keaktifan) Estimasi waktu: TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'		Network Security Infrastructure	1.43%
7	Kemampuan memahami cara kerja sistem komputer. (23-INF-SCPMK-0311)	Kemampuan dalam pemahaman konsep sistem operasi Windows dan Linux	Kriteria: Penguasaan Bentuk Penilaian:	Bentuk pembelajaran: Tatap muka di kelas		Windows Security & Linux Overview	1.43%

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

SPT-I/XXX/XXX

Issue/Revisi : A0

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)	
	Kemampuan yang diharapkan: Mampu memahami arsitektur dan konfigurasi sistem operasi serta alat administratif keamanan	serta administrasi keamanannya.	Forum	<u>Metode pembelajaran:</u> Ceramah Partisipasi (Keaktifan) <u>Estimasi waktu:</u> TM = 2 x 50' BM = 2 x 60' BS = 2 x 60'			
8	Evaluasi Tengah Semester : Melakukan validasi hasil penilaian, evaluasi dan perbaikan proses pembelajaran berikutnya (Bobot 30%)						
9	Kemampuan memahami cara kerja sistem komputer. (23-INF-SCPMK-0311) Kemampuan yang diharapkan: Mampu menggunakan alat perlindungan endpoint dan mitigasi malware	Kemampuan dalam Pemahaman terkait sistem pertahanan endpoint serta dampak malware.	Kriteria: Penguasaan Bentuk Penilaian: Forum			System and Endpoint Protection	1.43%
10	Kemampuan memahami cara kerja sistem komputer. (23-INF-SCPMK-0311) Kemampuan yang diharapkan: Mampu memahami strategi pertahanan mendalam dan manajemen keamanan siber	Kemampuan dalam Pemahaman strategi pertahanan jaringan dan kebijakan keamanan.	Kriteria: Penguasaan Bentuk Penilaian: Forum			Cybersecurity Principles, Practices, and Processes	1.43%

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

SPT-I/XXX/XXX

Issue/Revisi : A0

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)	
11	Kemampuan mengembangkan algoritma untuk memecahkan masalah. (23-INF-SCPMK-0322) Kemampuan yang diharapkan: Mampu mengimplementasikan berbagai aspek pertahanan sistem dan jaringan	Kemampuan dalam konfigurasi keamanan fisik, pengamanan aplikasi, dan segmentasi jaringan.	Kriteria: Penguasaan Bentuk Penilaian: Tugas			System and Network Defense	2.86%
12	Kemampuan menerapkan berbagai algoritma untuk memecahkan masalah. (23-INF-SCPMK-0323) Kemampuan yang diharapkan: Mampu mengonfigurasi dan mengelola kontrol akses jaringan	Kemampuan dalam Konfigurasi firewall berbasis kebijakan zona dan mitigasi serangan dengan ACL.	Kriteria: Penguasaan Kriteria: Penguasaan Bentuk Penilaian: Tugas			Firewall Technologies	2.86%
13	Kemampuan menganalisis persoalan computing yang kompleks. (23-INF-SCPMK-0411) Kemampuan yang diharapkan: Mampu memahami dan menerapkan keamanan cloud.	Kemampuan dalam analisis kebutuhan keamanan cloud dan implementasinya dalam skenario cloud nyata.	Kriteria: Penguasaan Bentuk Penilaian: Tugas			Cloud Security	2.86%

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)	
14	Kemampuan merancang algoritma untuk memecahkan masalah. (23-INF-SCPMK-0321) Kemampuan yang diharapkan: Mampu memahami dasar-dasar kriptografi dan autentikasi data	Kemampuan dalam penggunaan teknik enkripsi, hashing, dan tanda tangan digital.	Kriteria: Penguasaan Bentuk Penilaian: Forum			Cryptography	1.43%
15	Kemampuan menganalisis persoalan computing yang kompleks. (23-INF-SCPMK-0411) Kemampuan yang diharapkan: Mampu menggunakan teknik dan alat pemantauan keamanan jaringan	Kemampuan dalam evaluasi log keamanan, identifikasi ancaman, dan forensik digital.	Kriteria: Penguasaan Bentuk Penilaian: Tugas			Technologies and Protocols	2.86%
16	Evaluasi Akhir Semester: Melakukan validasi penilaian akhir dan menentukan kelulusan mahasiswa (Bobot 30%)						