RENCANA PEMBELAJARAN SEMESTER (RPS)
PROGRAM STUDI INFORMATIKA
INF515- IT FUNDAMENTALS FOR CYBERSECURITY

SPT-I/02/BPP-LSE/POB-01/F-01

Issue/Revisi : R1

Mata Kuliah	IT Fundamentals for Cybersecurity	Tanggal	04 Agustus 2025
Kode MK	INF515	Rumpun MK	MKP
Bobot (sks)	T (Teori) : 2 P (Praktik/Praktikum) : 1	Semester	7 (Tujuh)
Dosen Pengembang RPS,  (Hendi Hermawan, S.T., M.T.I.)	Koordinator Keilmuan,  (Mohammad Nasucha, Ph.D)	Kepala Program Studi,  (Dr. Ida Nurhaida, M.T)	Dekan  (Danto Sukmajati, Ph.D)

RENCANA PEMBELAJARAN SEMESTER		
Capaian Pembelajaran (CP)	**CPL – PRODI yang dibebankan pada MK**	
	CPL03	Memiliki kemampuan memahami (C2) cara kerja sistem komputer serta menerapkan (C3) berbagai algoritma/metode untuk memecahkan masalah dalam suatu organisasi.
	CPL08	Memiliki kemampuan untuk menentukan (C2) dan mengimplementasikan solusi (C3) berbasis computing yang sesuai dengan kebutuhan pengguna.
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	CPMK032	Mampu menerapkan (C3) berbagai metode/algoritma untuk memecahkan masalah dalam suatu organisasi.

RENCANA PEMBELAJARAN SEMESTER

CPMK081	Mampu mengidentifikasi kebutuhan computing pengguna dengan benar (C2).
CPMK082	Mampu menentukan solusi berbasis computing yang sesuai dengan kebutuhan pengguna (C2).
CPMK083	Mampu mengimplementasikan solusi berbasis computing yang sesuai dengan kebutuhan pengguna (C3)
Kemampuan Akhir Tiap Tahap Belajar (SCPMK)	
SCPMK0326	Mampu **menerapkan** pengetahuan-pengetahuan dalam ranah ***Cyber Security*** untuk memecahkan masalah.
SCPMK0819	Mampu mengidentifikasi kebutuhan computing pengguna dengan benar, **khususnya pada ranah terkait dengan metode/algoritma yang dipilih.**
SCPMK0829	Mampu **memilih solusi** yang sesuai dengan kebutuhan pengguna, khususnya yang terkait dengan ***Cyber Security.***
SCPMK0839	Mampu **mengimplementasikan solusi** untuk memecahkan masalah pengguna, khususnya dalam ranah ***Cyber Security.***

Korelasi CPMK terhadap SCPMK

	SCPMK0326	**SCPMK0819**	**SCPMK0829**	**SCPMK0839**
CPMK032	√			
CPMK081		√		
CPMK082			√	
CPMK083				√

RENCANA PEMBELAJARAN SEMESTER (RPS)
PROGRAM STUDI INFORMATIKA
INF515- IT FUNDAMENTALS FOR CYBERSECURITY

SPT-I/02/BPP-LSE/POB-01/F-01

Issue/Revisi : R1

RENCANA PEMBELAJARAN SEMESTER

Kode CPL	Kode CPMK	Kode Sub CPMK	Indikator	Metode Penilaian	Bobot
CPL03	CPMK032	SCPMK0326	Mampu menerapkan pengetahuan-pengetahuan dalam ranah Cyber Security untuk memecahkan masalah.	Kuis, studi kasus, diskusi, dan UTS (berbasis skenario).	20%
CPL08	CPMK081	SCPMK0819	Mampu mengidentifikasi kebutuhan computing pengguna dengan benar, khususnya pada ranah terkait dengan metode/algoritma yang dipilih.	Observasi diskusi, studi kebutuhan sistem, dan soal UTS.	15%
CPL08	CPMK082	SCPMK0829	Mampu memilih solusi yang sesuai dengan kebutuhan pengguna, khususnya yang terkait dengan Cyber Security.	Kuis, simulasi desain sistem, tugas studi kasus, tanya jawab.	20%
CPL08	CPMK083	SCPMK0839	Mampu mengimplementasikan solusi untuk memecahkan masalah pengguna, khususnya dalam ranah Cyber Security.	Praktikum, mini-proyek, analisis log keamanan, dan UAS (presentasi proyek).	45%

Deskripsi Singkat MK	Mata kuliah ini memfasilitasi mahasiswa dalam mempelajari dasar-dasar teknologi informasi dan konsep dasar keamanan siber. Fokus diberikan pada identifikasi kebutuhan pengguna, pemilihan solusi TI, dan penerapannya dalam konteks perlindungan data. Mahasiswa dibekali pemahaman awal untuk mendukung pengembangan solusi keamanan sistem secara komprehensif.
Bahan Kajian : Materi Pembelajaran/Pokok Bahasan	1. Pengantar Cyber Security dan Peran Teknologi Informasi 2. Jenis Ancaman Siber dan Vektor Serangan 3. Infrastruktur Jaringan dan Komponen Sistem Komputer 4. Konsep Keamanan Data dan Model CIA (Confidentiality, Integrity, Availability) 5. Identifikasi Kebutuhan Sistem Keamanan 6. Teknologi Pengamanan Jaringan dan Endpoint 7. Kontrol Akses, Firewall, dan IDS/IPS 8. Dasar-dasar Kriptografi dan Aplikasi Enkripsi 9. Analisis Risiko dan Kerentanan Sistem (Vulnerability Assessment) 10. Monitoring Sistem, Logging, dan Analisis Alert

RENCANA PEMBELAJARAN SEMESTER

11. Tanggap Insiden dan Dasar Digital Forensik
12. Pengenalan CVSS dan Penilaian Risiko Ancaman
13. Sistem SIEM dan Analisis Data Keamanan
14. Praktik Deteksi Anomali dan Investigasi Awal
15. Perancangan Solusi Keamanan Terapan

Pustaka

Utama

Cisco Networking Academy. (2020). Cybersecurity Operations (CyberOps) Associate v1.0 – Course Material. Cisco Press.

Ciampa, M. (2022). *Security+ Guide to Network Security Fundamentals* (7th ed.). Cengage Learning.

Pendukung

NIST. (2020). Framework for Improving Critical Infrastructure Cybersecurity – NIST SP 800-53.

Media Pembelajaran

Perangkat Lunak:	**Perangkat Keras:**
LMS Collabor Aplikasi IDE pemrograman Python (Jupyter Notebook)	Komputer/Laptop Internet LCD Proyektor

Dosen Pengampu: Hendi Hermawan

Mata Kuliah Prasyarat: -

Indikator, Kriteria, dan Bobot Penilaian

SCPMK	Penilaian dan Bobot					Total Bobot Penilaian
	Tugas 1	Tugas 2	Tugas 3	UTS	UAS (Proyek Akhir)	
	unjuk kerja (diskusi, tanya jawab, rancangan proyek)	unjuk kerja (diskusi, tanya jawab, rancangan proyek)	unjuk kerja (diskusi, tanya jawab, rancangan proyek)	Ujian Tertulis	unjuk kerja (diskusi, tanya jawab, presentasi proyek)	
SCPMK0321	5%	5%	-	10%	-	20%
SCPMK0811	5%	5%	-	5%	-	15%

RENCANA PEMBELAJARAN SEMESTER (RPS)
PROGRAM STUDI INFORMATIKA
INF515- IT FUNDAMENTALS FOR CYBERSECURITY

SPT-I/02/BPP-LSE/POB-01/F-01

Issue/Revisi : R1

RENCANA PEMBELAJARAN SEMESTER

SCPMK0821	5%	5%	5%	5%	-	20%
SCPMK0831	-	5%	10%	-	30%	45%
Total per penilaian	**15%**	**20%**	**15%**	**20%**	**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				
(1)	*(2)*	*(3)*	*(4)*	*Luring (5)*	*Daring (6)*	*(7)*	
1	SCPMK0321 Mampu menerapkan pengetahuan-pengetahuan dalam ranah Cyber Security untuk memecahkan masalah.	Mahasiswa mampu menjelaskan konsep dasar keamanan informasi termasuk prinsip CIA (Confidentiality, Integrity, Availability) dan pentingnya keamanan dalam sistem TI.	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Tanya jawab	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50' BM = 3 x 60' BS = 3 x 60'	-	The Danger – Threat Landscape, CIA Triad, Threat Actors, Threat Impact.	
2	SCPMK0321 Mampu menerapkan pengetahuan-pengetahuan dalam ranah Cyber Security untuk memecahkan masalah.	Mahasiswa mampu menjelaskan struktur organisasi keamanan informasi serta peran dan fungsi Security Operations Center (SOC).	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Tanya jawab	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50' BM = 3 x 60'		Security Operations Center, Defender Roles, Cybersecurity Career Path.	

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 = 3 x 60’			
3	SCPMK0811 Mampu mengidentifikasi kebutuhan computing pengguna, khususnya yang terkait dengan Cyber Security.	Mahasiswa mampu mengidentifikasi fitur keamanan sistem operasi Windows dan Linux serta potensi kerentanannya.	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Studi Kasus	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50’ BM = 3 x 60’ BS = 3 x 60’		Windows OS Overview, Linux Basics, File System, Shell, Log Files.	15%
4	SCPMK0811 Mampu mengidentifikasi kebutuhan computing pengguna, khususnya yang terkait dengan Cyber Security.	Mahasiswa mampu menjelaskan komunikasi jaringan, model OSI dan TCP/IP, serta penggunaan protokol dasar seperti IP, ICMP, ARP.	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Tanya jawab	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50’ BM = 3 x 60’ BS = 3 x 60’		OSI, Ethernet, IPv4/6, ARP, ICMP, Connectivity Tools.	
5	SCPMK0821 Mampu memilih solusi yang sesuai dengan kebutuhan pengguna, khususnya yang terkait dengan Cyber Security.	Mahasiswa mampu menganalisis fungsi protokol dan layanan seperti DNS, DHCP, NAT, dan HTTP serta kaitannya dengan keamanan.	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Tanya jawab	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi)		Network Services (DNS, DHCP, HTTP, NAT).	

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 = 3 x 50' BM = 3 x 60' BS = 3 x 60'			
6	SCPMK0821 Mampu memilih solusi yang sesuai dengan kebutuhan pengguna, khususnya yang terkait dengan Cyber Security.	Mahasiswa mampu menjelaskan berbagai jenis serangan siber, termasuk rekayasa sosial, malware, dan serangan jaringan.	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Tanya jawab	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50' BM = 3 x 60' BS = 3 x 60'		Network Attacks, Social Engineering, Malware, Threat Actors.	
7	SCPMK0321 Mampu menerapkan pengetahuan-pengetahuan dalam ranah Cyber Security untuk memecahkan masalah.	Mahasiswa mampu menjelaskan konsep defense-in-depth dan menerapkan kebijakan keamanan dasar.	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Studi Kasus	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50' BM = 3 x 60' BS = 3 x 60'		Defense-in-Depth, Policy Framework, Risk Management.	20%
8	**Evaluasi Tengah Semester : Melakukan validasi hasil penilaian, evaluasi dan perbaikan proses pembelajaran berikutnya (20%)**						
9	SCPMK0821 Mampu memilih solusi yang sesuai dengan kebutuhan pengguna, khususnya yang terkait dengan Cyber Security.	Mahasiswa mampu menjelaskan konsep dasar kriptografi, penggunaan enkripsi simetris dan asimetris, serta	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:**		Cryptography, Symmetric/Asymmetric, Hashing, PKI.	

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)*	
		PKI.kesehatan, keuangan, dan hukum.	**Bentuk penilaian:** Tanya jawab	Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50' BM = 3 x 60' BS = 3 x 60'			
10	SCPMK0831 Mampu mengimplementasikan solusi untuk memecahkan masalah pengguna, khususnya dalam ranah Cyber Security.	Menjelaskan dan mengimplementasikan kontrol akses serta mekanisme AAA (Authentication, Authorization, Accounting).	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Tanya jawab	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50' BM = 3 x 60' BS = 3 x 60'		Access Control, AAA Concepts, ACL, Identity Management.	
11	SCPMK0831 Mampu mengimplementasikan solusi untuk memecahkan masalah pengguna, khususnya dalam ranah Cyber Security.	Menjelaskan teknik perlindungan endpoint dan mengimplementasikan kebijakan endpoint security.	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Tanya jawab	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50' BM = 3 x 60' BS = 3 x 60'		Endpoint Security, Malware Detection, Host-based Prevention.	
12	SCPMK0831	Menjelaskan proses penilaian kerentanan sistem menggunakan CVSS dan	**Kriteria penilaian:**	**Bentuk pembelajaran:** Tatap muka di kelas		Vulnerability Assessment, CVSS, Risk Register.	15%

RENCANA PEMBELAJARAN SEMESTER (RPS)
PROGRAM STUDI INFORMATIKA
INF515- IT FUNDAMENTALS FOR CYBERSECURITY

SPT-I/02/BPP-LSE/POB-01/F-01

Issue/Revisi : R1

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)*	
	Mampu mengimplementasikan solusi untuk memecahkan masalah pengguna, khususnya dalam ranah Cyber Security.	mengelola kebijakan keamanan informasi.	Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Studi Kasus	**Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50' BM = 3 x 60' BS = 3 x 60'			
13	SCPMK0831 Mampu mengimplementasikan solusi untuk memecahkan masalah pengguna, khususnya dalam ranah Cyber Security.	Menjelaskan metode pengumpulan, penyimpanan, dan analisis log keamanan untuk mendeteksi anomali jaringan.	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Tanya jawab	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50' BM = 3 x 60' BS = 3 x 60'		Network Monitoring, Log Analysis, SIEM Introduction.	
14	SCPMK0831 Mampu mengimplementasikan solusi untuk memecahkan masalah pengguna, khususnya dalam ranah Cyber Security.	Melakukan analisis alert keamanan dan menyusun respons insiden awal berdasarkan data monitoring.	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Tanya jawab	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50' BM = 3 x 60' BS = 3 x 60'		Alert Analysis, Threat Intelligence, Incident Response Plan.	

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)*	
15	SCPMK0831 Mampu mengimplementasikan solusi untuk memecahkan masalah pengguna, khususnya dalam ranah Cyber Security.	Menjelaskan prinsip digital forensic, cyber kill chain, dan langkah-langkah investigasi siber.	**Kriteria penilaian:** Ketepatan dalam menjelaskan serta penguasaan **Bentuk penilaian:** Tanya jawab	**Bentuk pembelajaran:** Tatap muka di kelas **Metode pembelajaran:** Ceramah Partisipasi (kemampuan literasi) **Estimasi waktu:** TM = 3 x 50' BM = 3 x 60' BS = 3 x 60'		Digital Forensics, Kill Chain, Incident Triage.	
16	**Evaluasi Akhir Semester: Melakukan validasi penilaian akhir dan menentukan kelulusan mahasiswa (30%)**						