	UNIVERSITAS LEMBAH DEMPO **FAKULTAS SAINS & TEKNOLOGI** PROGRAM STUDI SISTEM INFORMASI **RENCANA PEMBELAJARAN SEMESTER (RPS)**	Kode Dokumen **RPS/IF-3501/2026/001**

MATA KULIAH (MK)	**KODE MK**	**RUMPUN MK**	**BOBOT (sks)**	**SEMESTER**	**TGL PENYUSUNAN**
Keamanan Sistem	MWM217308	Sistem Informasi / SE	3 SKS	7	2026-09-28
OTORISASI / PENGESAHAN	**Pengembang RPS**		**Koordinator RMK**		**Ketua Program Studi**
Tanda Tangan & Cap *(Pengesahan Resmi)*	YUNIANSYAH				M. Junius Effendi., M.Kom

CAPAIAN PEMBELAJARAN (CP)

CPL-PRODI yang Dibebankan pada MK	**Deskripsi CPL**
ku1 (Keterampilan Umum)	Mampu berpikir logis, kritis, sistematis, kreatif, inovatif, serta mengambil keputusan berdasarkan analisis data dan metode ilmiah dalam menyelesaikan permasalahan Sistem Informasi.
ku2 (Keterampilan Umum)	Mampu berkomunikasi secara efektif, bekerja sama dalam tim multidisiplin, menyusun karya ilmiah, serta memanfaatkan teknologi informasi secara profesional.
kk1 (Keterampilan Khusus)	Mampu menganalisis kebutuhan organisasi serta merancang solusi Sistem Informasi yang mendukung proses bisnis, pengambilan keputusan, dan transformasi digital.
kk2 (Keterampilan Khusus)	Mampu mengembangkan, mengimplementasikan, mengintegrasikan, menguji, dan mengevaluasi aplikasi berbasis web, mobile, multimedia, serta teknologi digital sesuai kebutuhan pengguna.
kk3 (Keterampilan Khusus)	Mampu merancang, mengelola, mengamankan basis data, menerapkan analitik data dan kecerdasan buatan untuk menghasilkan informasi yang mendukung pengambilan keputusan organisasi.

pp1 (Pengetahuan)	Menguasai konsep, teori, prinsip, dan metodologi Sistem Informasi yang mengintegrasikan aspek teknologi informasi, proses bisnis, manajemen, dan organisasi.
pp2 (Pengetahuan)	Menguasai metode analisis, perancangan, pengembangan, implementasi, pengujian, evaluasi, tata kelola, keamanan, dan manajemen proyek Sistem Informasi.
pp3 (Pengetahuan)	Menguasai konsep basis data, analitik data, kecerdasan buatan, multimedia, teknologi web, teknologi mobile, dan teknologi digital terkini untuk mendukung transformasi digital organisasi.
s2 (Sikap)	Bersikap profesional, adaptif, mampu bekerja sama, berkomunikasi secara efektif, memiliki jiwa kepemimpinan, kewirausahaan, serta berkomitmen pada pembelajaran sepanjang hayat.
Capaian Pembelajaran Mata Kuliah (CPMK)	**Deskripsi CPMK & Sub-CPMK Turunan**
CPMK-215	**Mampu menjelaskan konsep, prinsip, ancaman, kerentanan, mekanisme perlindungan, dan aspek keamanan Sistem Informasi.** • **Sub-CPMK-215.1**: Menjelaskan konsep, tujuan, prinsip, dan aspek keamanan Sistem Informasi. (15.00%) • **Sub-CPMK-215.2**: Menjelaskan berbagai jenis ancaman, kerentanan, dan serangan terhadap sistem. (15.00%) • **Sub-CPMK-215.3**: Menjelaskan mekanisme perlindungan terhadap sistem, aplikasi, data, dan akses pengguna. (15.00%)
CPMK-216	**Mampu menganalisis ancaman, kerentanan, risiko, dan kebutuhan keamanan pada Sistem Informasi dan infrastruktur teknologi.** • **Sub-CPMK-216.1**: Mengidentifikasi aset, ancaman, dan kerentanan pada Sistem Informasi dan infrastruktur. (15.00%) • **Sub-CPMK-216.2**: Menganalisis risiko keamanan berdasarkan kemungkinan dan dampak ancaman. (15.00%) • **Sub-CPMK-216.3**: Menganalisis kebutuhan keamanan berdasarkan karakteristik sistem dan organisasi. (15.00%) • **Sub-CPMK-216.4**: Menentukan prioritas kebutuhan pengamanan berdasarkan tingkat risiko. (15.00%)
CPMK-217	**Mampu menerapkan mekanisme keamanan yang sesuai untuk melindungi sistem, aplikasi, data, dan akses pengguna berdasarkan kebutuhan keamanan.** • **Sub-CPMK-217.1**: Menerapkan mekanisme autentikasi dan otorisasi untuk pengamanan akses sistem. (15.00%) • **Sub-CPMK-217.2**: Menerapkan mekanisme perlindungan data dan komunikasi sesuai kebutuhan keamanan. (15.00%) • **Sub-CPMK-217.3**: Menerapkan pengendalian keamanan pada aplikasi, sistem, atau infrastruktur. (15.00%) • **Sub-CPMK-217.4**: Mendokumentasikan konfigurasi dan mekanisme keamanan yang diterapkan. (15.00%)

CPMK-218	**Mampu mengevaluasi tingkat keamanan Sistem Informasi berdasarkan hasil identifikasi risiko, pengujian keamanan, pengendalian, dan kebutuhan organisasi.** • **Sub-CPMK-218.1**: Menentukan indikator dan parameter evaluasi keamanan Sistem Informasi. (15.00%) • **Sub-CPMK-218.2**: Melakukan pengujian terhadap mekanisme keamanan yang diterapkan. (15.00%) • **Sub-CPMK-218.3**: Mengevaluasi tingkat keamanan sistem berdasarkan hasil analisis risiko dan pengujian. (15.00%) • **Sub-CPMK-218.4**: Menyusun rekomendasi peningkatan keamanan berdasarkan hasil evaluasi. (15.00%)

DESKRIPSI MATA KULIAH & BAHAN KAJIAN

Deskripsi Singkat MK	Mata kuliah ini membekali mahasiswa dengan pemahaman konsep, teknik, dan praktik keamanan sistem informasi secara komprehensif, mencakup identifikasi ancaman dan kerentanan, manajemen risiko, penerapan kriptografi, mekanisme kontrol akses, penyusunan kebijakan dan audit keamanan, keamanan jaringan dan aplikasi web, deteksi dan respon insiden, hingga strategi backup dan disaster recovery. Pembelajaran menekankan pendekatan Outcome Based Education (OBE) melalui kombinasi ceramah, diskusi, studi kasus, praktikum, dan proyek akhir
Bahan Kajian (BK) / Materi Pembelajaran	1. **BK7** - Infrastructure, Platform and Security (Bobot Min: 0.00%) - Metode analisis kebutuhan, pemodelan sistem, desain, serta implementasi solusi berbasis teknologi informasi. 2. **BK9** - Emerging Technologies (AI, IoT, Mobile, Cloud) (Bobot Min: 0.00%) - Manajemen keamanan informasi, privasi data, pengendalian risiko, serta kepatuhan terhadap regulasi.
Pustaka / Referensi	**Utama:** 1. Victor Benny Alexsius Pardosi, Bernadete Deta, Fifto Nugroho, dan Arnes Yuli Vandika (2024). *Keamanan Sistem Informasi*. PT MAFY MEDIA LITERASI INDONESIA. 2. Dr. Budi Raharjo, S.Kom., M.Kom., MM (2021). *KEAMANAN SISTEM INFORMASI*. Yayasan Prima Agus Teknik.
Dosen Pengampu	YUNIANSYAH, S.Kom, M.Kom (NIDN: 0228067001)

RENCANA KEGIATAN PEMBELAJARAN MINGGUAN (16 PERTEMUAN)

Mg Ke-	Sub-CPMK (Kemampuan Akhir)	Materi Pembelajaran	Bentuk & Metode Pembelajaran	Estimasi Waktu	Indikator & Assessment	Bobot (%)

1	Sub-CPMK-215.1 Menjelaskan konsep, tujuan, prinsip, dan aspek keamanan Sistem Informasi.	Konsep Dasar Keamanan Sistem: pengertian, tujuan, prinsip CIA Triad, aset informasi, konteks keamanan siber vs keamanan informasi	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50")	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-1	**3.00%**
2	Sub-CPMK-215.2 Menjelaskan berbagai jenis ancaman, kerentanan, dan serangan terhadap sistem.	Ancaman Sistem: taksonomi ancaman, threat actor, malware, social engineering	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50")	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-2	**3.00%**
3	Sub-CPMK-215.3 Menjelaskan mekanisme perlindungan terhadap sistem, aplikasi, data, dan akses pengguna.	Serangan & Kerentanan Sistem: jenis serangan (DoS/DDoS, MITM, injection, dsb.), analisis kerentanan (vulnerability analysis), studi kasus insiden nyata	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50")	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-3	**3.00%**
4	Sub-CPMK-216.2 Menganalisis risiko keamanan berdasarkan kemungkinan dan dampak ancaman.	Manajemen Risiko Keamanan Informasi: identifikasi aset & risiko, analisis kualitatif/kuantitatif, evaluasi, strategi mitigasi, kerangka ISO 31000/27005	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50"); PT: 1x(2x60"); BM: 1x(2x60")	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-4	**3.00%**
5	Sub-CPMK-216.3 Menganalisis kebutuhan keamanan berdasarkan karakteristik sistem dan organisasi.	Kriptografi Dasar: sejarah singkat, kriptografi simetris (DES, AES), kriptografi asimetris (RSA, ECC), manajemen kunci	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50")	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-5	**5.00%**
6	Sub-CPMK-217.1 Menerapkan mekanisme autentikasi dan otorisasi untuk pengamanan akses sistem.	Penerapan Kriptografi: fungsi hash (SHA), tanda tangan digital, sertifikat digital & Public Key Infrastructure (PKI), SSL/TLS	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50")	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-6	**5.00%**

7	Sub-CPMK-216.4 Menentukan prioritas kebutuhan pengamanan berdasarkan tingkat risiko.	Mekanisme Kontrol Akses: autentikasi, otorisasi, DAC, MAC, RBAC, ABAC, autentikasi multifaktor (MFA), Single Sign-On	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50")	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-7	**3.00%**
8	Sub-CPMK-216.4 Menentukan prioritas kebutuhan pengamanan berdasarkan tingkat risiko.	Materi Pertemuan 1 - 7	Ujian / Evaluasi Terstruktur	TM: 1x(2x50");	**Assessment:** UTS Evaluasi Capaian Pembelajaran Minggu 1-7	**20.00%**
9	Sub-CPMK-217.3 Menerapkan pengendalian keamanan pada aplikasi, sistem, atau infrastruktur.	Kebijakan & Prosedur Keamanan Informasi: struktur kebijakan, SOP, kepatuhan (compliance), kerangka ISO/IEC 27001	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50")	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-9	**3.00%**
10	Sub-CPMK-217.3 Menerapkan pengendalian keamanan pada aplikasi, sistem, atau infrastruktur.	Audit & Penilaian Sistem Keamanan: jenis audit (internal/eksternal), metodologi audit, penilaian kematangan keamanan (maturity assessment), pelaporan temuan	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50")	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-10	**3.00%**
11	Sub-CPMK-217.4 Mendokumentasikan konfigurasi dan mekanisme keamanan yang diterapkan.	Keamanan Jaringan: firewall, IDS/IPS, VPN, segmentasi jaringan, keamanan nirkabel	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50");	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-11	**5.00%**
12	Sub-CPMK-217.2 Menerapkan mekanisme perlindungan data dan komunikasi sesuai kebutuhan keamanan.	Keamanan Aplikasi Web: OWASP Top 10 (SQL Injection, XSS, dsb.), secure coding practice	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50")	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-12	**5.00%**

13	Sub-CPMK-218.1 Menentukan indikator dan parameter evaluasi keamanan Sistem Informasi.	Sistem Deteksi & Respon Insiden: SIEM, deteksi anomali, tahapan incident response (persiapan, deteksi, containment, eradication, recovery, lesson learned)	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50");	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-13	**5.00%**
14	Sub-CPMK-218.4 Menyusun rekomendasi peningkatan keamanan berdasarkan hasil evaluasi.	Strategi Backup & Disaster Recovery: jenis backup, RTO & RPO, Disaster Recovery Plan (DRP), Business Continuity Plan (BCP)	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50");	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-14	**3.00%**
15	Sub-CPMK-218.4 Menyusun rekomendasi peningkatan keamanan berdasarkan hasil evaluasi.	Integrasi seluruh materi Bab 1–10 dalam studi kasus komprehensif keamanan sistem informasi organisasi	Kuliah, Diskusi, & Praktikum	TM: 1x(2x50");	**Assessment:** Tugas / Quiz Pemahaman konsep dasar materi minggu ke-15	**3.00%**
16	Sub-CPMK-218.4 Menyusun rekomendasi peningkatan keamanan berdasarkan hasil evaluasi.	Materi Pertemuan 9 - 15	Ujian / Evaluasi Terstruktur	TM: 1x(2x50");	**Assessment:** UAS Evaluasi Capaian Pembelajaran Minggu 9-15	**20.00%**