	Universitas Negeri Surabaya S1 Teknik Informatika	Kode Dokumen

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (sks)	SEMESTER	Tgl Penyusunan
Keamanan Data dan Informasi	5520203140		3		25 Agustus 2026

OTORISASI	Pengembang RPS	Koordinator RMK	Koordinator Program Studi
			PARAMITHA NERISAFITRA

Deskripsi Singkat MK	Mata kuliah Keamanan Data dan Informasi membahas konsep fundamental, prinsip, dan praktik keamanan informasi yang mencakup aspek kerahasiaan, integritas, dan ketersediaan data. Mahasiswa dibekali pemahaman konseptual dan keterampilan praktis dalam penerapan kriptografi, keamanan jaringan dan sistem, serta manajemen risiko keamanan informasi untuk mendukung penyelenggaraan sistem informasi yang andal, bertanggung jawab, dan berkelanjutan dalam konteks pendidikan, industri, dan institusi publik.	
Capaian Pembelajaran (CP)	**CPL-PRODI yang dibebankan pada MK**	
	CPL-1	Mampu menunjukkan nilai-nilai agama, kebangsaan dan budaya nasional, serta etika akademik dalam melaksanakan tugasnya
	CPL-8	Mampu mengimplementasikan kebutuhan computing dengan mempertimbangkan berbagai metode/algoritma yang sesuai (COM-03)
	CPL-11	Mampu menganalisis persoalan computing yang kompleks untuk mengidentifikasi solusi pengelolaan proyek teknologi bidang informatika/ilmu komputer dengan mempertimbangkan wawasan perkembangan ilmu trandisiplin (KNO-01)
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	CPMK-1	Mampu menunjukkan (A3) sikap profesional dan etis dalam praktik keamanan informasi, serta bertanggung jawab atas hasil analisis dan rekomendasi yang diberikan.
	CPMK-2	Mampu merancang (C6) dan menerapkan (C3) mekanisme kriptografi simetris dan asimetris untuk proteksi data at-rest dan in-transit menggunakan algoritma standar.
	CPMK-3	Mampu menganalisis (C4) prinsip-prinsip fundamental keamanan informasi—mencakup kerahasiaan (confidentiality), integritas (integrity), ketersediaan (availability), otentikasi, dan non-repudiasi—dalam berbagai konteks sistem teknologi informasi.
	CPMK-4	Mampu mengevaluasi (C5) postur keamanan jaringan dan sistem menggunakan perangkat standar industri serta merekomendasikan kontrol teknis untuk mitigasi kerentanan yang teridentifikasi.
	CPMK-5	Mampu menganalisis (C4) risiko keamanan informasi dan menyusun elemen-elemen kebijakan keamanan berdasarkan kerangka kerja internasional seperti ISO/IEC 27001 dan NIST Cybersecurity Framework.
	Matrik CPL - CPMK	

CPMK	CPL-1	CPL-8	CPL-11
CPMK-1	✔		
CPMK-2		✔	
CPMK-3			✔
CPMK-4			✔
CPMK-5			✔

Matrik CPMK pada Kemampuan akhir tiap tahapan belajar (Sub-CPMK)

CPMK	Minggu Ke															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
CPMK-1															✔	✔
CPMK-2		✔	✔	✔	✔	✔										
CPMK-3	✔															
CPMK-4									✔	✔	✔	✔				
CPMK-5							✔	✔					✔	✔		

Pustaka

Utama :

1. Stallings, William. (2020). Cryptography and Network Security: Principles and Practice (8th Edition). Pearson.
2. William Stallings. 2017. Network Security Essentials : Applications and Standards Sixth edition Global edition. Pearson
3. Joseph Migga Kizza. 2020. Guide to Computer Network Security Fifth Edition. Springer.
4. Forouzan, Behrouz A., & Mukhopadhyay, Debdeep. (2015). Cryptography and Network Security (3rd Edition). McGraw-Hill.
5. International Organization for Standardization. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
6. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce

Pendukung :

Mg Ke-	Kemampuan akhir tiap tahapan belajar (Sub-CPMK)	Penilaian		Bentuk Pembelajaran, Metode Pembelajaran, Penugasan Mahasiswa, [Estimasi Waktu]		Materi Pembelajaran	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk	Luring (*offline*)	*Daring (online)*		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Mahasiswa mampu menjelaskan konsep fundamental keamanan informasi, arsitektur keamanan OSI, dan prinsip-prinsip desain keamanan.	Ketepatan dalam mendefinisikan CIA, ancaman, serangan, dan mekanisme keamanan.	Pemahaman konseptual yang benar. Bentuk: Partisipasi kelas, kuis formatif (tidak dinilai).	Ceramah Interaktif, Diskusi Kelompok. Membaca Stallings Bab 1.			
2	Mahasiswa mampu menjelaskan dan menerapkan algoritma kriptografi klasik (substitusi dan transposisi) untuk enkripsi/dekripsi pesan sederhana	Ketepatan dalam menerapkan Caesar Cipher, Vigenère Cipher, dan Rail Fence Cipher; Kemampuan menganalisis frekuensi huruf.	Logika penerapan algoritma benar, hasil enkripsi/dekripsi akurat. Bentuk: Kuis, Latihan Terstruktur.	Ceramah, Latihan Terbimbing. Mengerjakan soal latihan, membaca Stallings Bab 2-3.			5%
3	Mahasiswa mampu menjelaskan struktur block cipher modern dan prinsip kerja Data Encryption Standard (DES) dan Advanced Encryption Standard	Kemampuan menjelaskan struktur Feistel, putaran (rounds) pada DES, dan struktur SPN pada AES.	Pemahaman alur proses enkripsi DES dan AES. Bentuk: Kuis.	Ceramah, Studi Kasus (Evolusi dari DES ke AES). Membaca Stallings Bab 4, 6.			5%
4	Mahasiswa mampu menerapkan mode operasi block cipher (ECB, CBC, CFB, OFB, CTR) sesuai dengan kebutuhan aplikasi	Ketepatan dalam memilih mode operasi untuk skenario tertentu (misal, enkripsi file vs. streaming data).	Justifikasi pemilihan mode operasi logis dan benar. Bentuk: Latihan Terstruktur, bagian dari Laporan Praktikum.	Praktikum Terbimbing 1: Enkripsi File dengan AES			5%

5	Mahasiswa mampu menjelaskan konsep matematika dasar (Teori Bilangan dan Finite Fields) yang mendasari kriptografi kunci publik.	Kemampuan menghitung invers modular menggunakan Extended Euclidean Algorithm; Memahami Teorema Euler dan Fermat.	Ketepatan perhitungan matematis. Bentuk: Kuis, Latihan Terstruktur.	Ceramah, Latihan Soal. Mengerjakan soal latihan, membaca Stallings Bab 2, 5.			5%
6	Mahasiswa mampu menjelaskan dan menerapkan algoritma kriptografi kunci publik RSA dan skema pertukaran kunci Diffie-Hellman	1. Ketepatan dalam melakukan proses pembangkitan kunci, enkripsi, dan dekripsi menggunakan RSA 2. Menghitung kunci sesi bersama dengan Diffie-Hellman.	Alur perhitungan benar, hasil akurat. Bentuk: Kuis, Latihan Terstruktur.	Ceramah, Demonstrasi Perhitungan. Membaca Stallings Bab 9.			5%
7	Mahasiswa mampu menjelaskan fungsi dan aplikasi digital signature, fungsi hash, dan MAC untuk menjamin integritas dan otentikasi data.	Kemampuan membedakan antara enkripsi, hash, dan signature; Menjelaskan cara kerja HMAC.	Pemahaman konseptual yang jelas dan mampu memberikan contoh. Bentuk: Partisipasi Diskusi, Studi Kasus.	Ceramah Interaktif, Studi Kasus (Proses validasi update software). Membaca Stallings Bab 11, 12, 13.			5%
8	Mengukur penguasaan materi dari pertemuan 1 hingga 7.	Sesuai dengan kunci jawaban dan rubrik penilaian soal. Bentuk: Ujian Tulis (Esai, Studi Kasus Pendek).	Sesuai dengan kunci jawaban dan rubrik penilaian soal. Bentuk: Ujian Tulis (Esai, Studi Kasus Pendek).	Project Penugasan Kelompok			15%
9	Mahasiswa mampu menggunakan Nmap untuk melakukan pemindaian port, identifikasi layanan, dan deteksi sistem operasi pada jaringan target	1. Kemampuan menggunakan sintaks Nmap yang tepat (SYN scan, version scan, OS detection); Ketepatan interpretasi output Nmap. 2. Ketepatan interpretasi output Nmap.	Laporan praktikum menunjukkan pemahaman prosedur dan analisis hasil. Bentuk: Laporan Praktikum.	Praktikum Terbimbing 2: Network Discovery & Scanning.			5%
10	Mahasiswa mampu menggunakan Wireshark untuk menangkap dan menganalisis lalu lintas jaringan untuk mengidentifikasi protokol dan potensi anomali keamanan	1. Kemampuan menggunakan filter display 2. Mengidentifikasi kredensial tidak terenkripsi (HTTP, FTP) 3. Menganalisis three-way handshake TCP	Laporan praktikum berisi temuan yang relevan dan analisis yang tajam. Bentuk: Laporan Praktikum.	Praktikum Terbimbing : Analisis Protokol Jaringan.			5%
11	Mahasiswa mampu menjelaskan konsep dan arsitektur Firewall dan Intrusion Detection/Prevention Systems (IDS/IPS)	1. Kemampuan membedakan antara packet filtering, stateful inspection, dan proxy firewall 2. Menjelaskan perbedaan antara IDS dan IPS.	Pemahaman arsitektur dan fungsi masing-masing teknologi. Bentuk: Studi Kasus, Diskusi.	Case-based Learning, Diskusi. Membaca Stallings Bab 20.			5%
12	Mahasiswa mampu mengidentifikasi dan menjelaskan jenis-jenis kerentanan perangkat lunak umum (buffer overflow, SQL injection) dan malicious software	1. Kemampuan menjelaskan cara kerja serangan buffer overflow dan SQL injection 2. Mengklasifikasikan malware.	Pemahaman mekanisme serangan dan dampaknya. Bentuk: Kuis, Presentasi Kelompok.	Ceramah, Video Demonstrasi Serangan. Membaca Stallings Bab 21, Proyek Akhir			5%

13	Mahasiswa mampu menjelaskan proses manajemen risiko keamanan informasi dan komponen utama dari sebuah kebijakan keamanan	1. Kemampuan menjelaskan siklus manajemen risiko (identify, assess, treat, monitor) 2. Mengidentifikasi elemen-elemen penting dalam dokumen kebijakan.	Pemahaman proses dan struktur dokumen. Bentuk: Diskusi, Pengerjaan Proyek Akhir.	Problem-based Learning. Membaca materi ISO 27001 & NIST CSF, Proyek Akhir			5%
14	Mahasiswa mampu menjelaskan kerangka kerja keamanan ISO/IEC 27001 dan NIST CSF serta aspek etika dan hukum dalam keamanan siber	1. Kemampuan menjelaskan tujuan dan struktur ISO 27001 Annex A dan 5 fungsi NIST CSF 2. Membedakan antara tindakan etis dan ilegal.	Pemahaman tujuan dan struktur kerangka kerja. Bentuk: Presentasi Proyek Akhir, Diskusi.	Presentasi Proyek Akhir. Finalisasi Laporan Proyek Akhir.			10%
15	Presentasi Proyek Akhir dan Ulasan	1. Kemampuan mempresentasikan hasil analisis secara jelas, logis, dan persuasif 2. Kemampuan menjawab pertanyaan dari dosen dan audiens.	Sesuai dengan rubrik penilaian presentasi. Bentuk: Presentasi Kelompok.	simulasi, diskusi			10%
16	Capstone Project Akhir Semester	Mengukur penguasaan materi dari pertemuan 9 hingga 14 dan kemampuan integratif.	Ketepatan dalam menjawab soal	simulasi, diskusi			10%

SDGS (Sustainable Development Goals)



Catatan

1. **Capaian Pembelajaran Lulusan Program Studi (CPL-Prodi)** adalah rumusan kemampuan yang harus dimiliki oleh lulusan program studi yang mencakup sikap, penguasaan pengetahuan, keterampilan umum, dan keterampilan khusus sesuai dengan jenjang kualifikasi, yang diperoleh melalui proses pembelajaran.
2. **CPL-Prodi yang dibebankan pada Mata Kuliah** adalah bagian dari CPL-Prodi yang dipilih dan relevan untuk dikembangkan melalui suatu mata kuliah, sebagai dasar perumusan capaian pembelajaran mata kuliah.
3. **Capaian Pembelajaran Mata Kuliah (CPMK)** adalah kemampuan yang dirumuskan secara spesifik dan diturunkan dari CPL-Prodi yang dibebankan pada mata kuliah, serta menggambarkan kompetensi yang harus dicapai mahasiswa setelah menyelesaikan mata kuliah.
4. **Sub-CPMK** adalah kemampuan akhir yang direncanakan pada setiap tahap pembelajaran, sebagai penjabaran lebih rinci dari CPMK, bersifat terukur dan dapat diamati sesuai dengan materi pembelajaran.
5. **Indikator Penilaian** adalah pernyataan spesifik dan terukur yang digunakan untuk menilai ketercapaian Sub-CPMK, baik dari proses maupun hasil belajar mahasiswa, yang didukung dengan bukti penilaian.
6. **Kriteria Penilaian** adalah tolok ukur yang digunakan untuk menentukan tingkat ketercapaian hasil belajar mahasiswa berdasarkan indikator penilaian, guna menjamin penilaian yang objektif, konsisten, dan adil. Kriteria penilaian dapat bersifat kuantitatif dan/atau kualitatif.
7. **Bentuk Penilaian** meliputi penilaian tes dan non-tes sesuai dengan karakteristik capaian pembelajaran.
8. **Bentuk Pembelajaran** meliputi kuliah, responsi, tutorial, seminar atau bentuk lain yang setara, praktikum, praktik studio, praktik bengkel, praktik lapangan, penelitian, dan pengabdian kepada masyarakat.
9. **Metode Pembelajaran** merupakan cara penyampaian pembelajaran yang digunakan untuk mencapai capaian pembelajaran, antara lain Small Group Discussion, Project Based Learning, Case Based Learning, Collaborative Learning, Discovery Learning, Self-Directed Learning, serta metode lain yang relevan.
10. **Materi Pembelajaran** adalah bahan kajian yang disusun secara sistematis dalam bentuk pokok dan sub-pokok bahasan untuk mendukung pencapaian Sub-CPMK.
11. **Bobot Penilaian** adalah persentase kontribusi setiap komponen penilaian terhadap nilai akhir mata kuliah, yang ditetapkan secara proporsional sesuai tingkat kompleksitas dan ketercapaian Sub-CPMK, dengan total keseluruhan sebesar 100%.
12. TM = Tatap Muka, PT = Penugasan Terstruktur, BM = Belajar Mandiri.