RUBRIK PENILAIAN RENCANA PEMBELAJARAN SEMESTER (RPS)
MATA KULIAH KEAMANAN SISTEM INFORMASI (ISY3210) – 2 SKS TEORI
Program Studi D3-Manajemen Informatika Politeknik Negeri Padang

---

A. RUBRIK UMUM TUGAS PER PERTEMUAN

Rubrik ini digunakan sebagai acuan penilaian untuk setiap tugas pada pertemuan 1-7 dan 9-15. Setiap tugas memiliki bobot 2% atau 2.5% dengan rentang nilai 0-100. Nilai akhir tugas = (Skor total / 100) × Bobot tugas.

Kriteria	Bobot Kriteria	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Ketepatan Analisis	40%	Analisis sangat tepat, komprehensif, mendalam, mengaitkan dengan konsep dan studi kasus relevan, serta menunjukkan pemahaman tingkat tinggi	Analisis tepat dan cukup mendalam dengan sebagian besar konsep terkait, namun kurang eksplorasi	Analisis cukup tepat namun kurang mendalam, beberapa konsep tidak terkait atau kurang relevan	Analisis tidak tepat, dangkal, atau tidak sesuai dengan konsep
Kelengkapan	30%	Semua elemen tugas diselesaikan dengan lengkap, terstruktur, dan memenuhi semua instruksi	Sebagian besar elemen tugas diselesaikan dengan cukup lengkap, memenuhi sebagian besar instruksi	Beberapa elemen tugas tidak diselesaikan atau kurang lengkap, instruksi tidak sepenuhnya diikuti	Banyak elemen tugas tidak diselesaikan, instruksi diabaikan
Sistematika dan Bahasa	30%	Penyajian sangat sistematis, bahasa jelas, formal, mudah dipahami, dan bebas dari kesalahan tata bahasa	Penyajian sistematis, bahasa cukup jelas dan formal dengan sedikit kesalahan tata bahasa	Penyajian kurang sistematis, bahasa kurang jelas, terdapat beberapa kesalahan tata bahasa	Penyajian tidak sistematis, bahasa tidak jelas, banyak kesalahan tata bahasa

---

B. RUBRIK KHUSUS PER PERTEMUAN

Pertemuan 1: Sub-CPMK 1.1 – Prinsip CIA Triad (Bobot 2%)

Tugas: Analisis studi kasus kebocoran data dan identifikasi pelanggaran CIA

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Identifikasi Pelanggaran CIA	Kemampuan mengidentifikasi aspek kerahasiaan, integritas, dan ketersediaan dalam kasus	Mengidentifikasi dengan tepat ketiga aspek CIA, disertai bukti dan penjelasan mendalam	Mengidentifikasi ketiga aspek dengan tepat namun kurang detail	Hanya mengidentifikasi 1-2 aspek dengan benar	Tidak dapat mengidentifikasi atau salah identifikasi
Analisis Dampak	Kemampuan menganalisis dampak pelanggaran terhadap organisasi dan pengguna	Analisis dampak komprehensif mencakup aspek finansial, reputasi, operasional, dan hukum	Analisis dampak mencakup 2-3 aspek dengan cukup baik	Analisis dampak hanya mencakup 1 aspek secara sederhana	Tidak ada analisis dampak atau tidak relevan
Rekomendasi Dasar	Kemampuan memberikan rekomendasi perbaikan sederhana	Memberikan 3+ rekomendasi yang relevan, spesifik, dan dapat ditindaklanjuti	Memberikan 2 rekomendasi yang cukup relevan	Memberikan 1 rekomendasi yang kurang spesifik	Tidak memberikan rekomendasi

Pertemuan 2: Sub-CPMK 1.2 – Ancaman dan Kerentanan (Bobot 2%)

Tugas: Analisis kasus serangan siber dan pembuatan peta ancaman

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Identifikasi Ancaman	Kemampuan mengidentifikasi jenis ancaman dan modus serangan	Mengidentifikasi 5+ ancaman dengan deskripsi modus operandi yang detail dan akurat	Mengidentifikasi 3-4 ancaman dengan deskripsi cukup jelas	Mengidentifikasi 1-2 ancaman dengan deskripsi minimal	Tidak dapat mengidentifikasi ancaman
Peta Ancaman	Kualitas pembuatan peta ancaman (threat map)	Peta ancaman komprehensif mencakup vektor serangan, aset terdampak, tingkat risiko, dan mitigasi awal	Peta ancaman cukup lengkap mencakup sebagian besar elemen	Peta ancaman sederhana dengan beberapa elemen	Peta ancaman tidak lengkap atau tidak sesuai
Keterkaitan dengan Organisasi	Kemampuan mengaitkan ancaman dengan konteks organisasi tertentu	Menjelaskan secara mendalam bagaimana ancaman berdampak pada organisasi spesifik (UKM, rumah sakit, bank)	Menjelaskan dampak secara umum tanpa konteks spesifik	Kurang mampu mengaitkan dengan konteks organisasi	Tidak ada kaitan dengan konteks organisasi

Pertemuan 3: Sub-CPMK 1.3 – Standar Keamanan Informasi (Bobot 2.5%)

Tugas: Analisis perbandingan ISO 27001 dan NIST Cybersecurity Framework

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Pemahaman Struktur Standar	Kemampuan menjelaskan struktur ISO 27001 (14 domain) dan NIST (5 functions)	Menjelaskan secara rinci dan akurat kedua standar beserta komponennya	Menjelaskan dengan cukup baik namun ada sedikit kekurangan	Menjelaskan secara umum tanpa detail	Tidak dapat menjelaskan atau salah
Analisis Perbandingan	Kualitas perbandingan antara kedua standar	Perbandingan komprehensif mencakup 5+ aspek (pendekatan, fokus, implementasi, sertifikasi, dll) dengan analisis mendalam	Perbandingan mencakup 3-4 aspek dengan analisis cukup	Perbandingan sederhana 1-2 aspek dengan analisis dasar	Perbandingan tidak lengkap atau tidak relevan
Rekomendasi Penggunaan	Kemampuan merekomendasikan standar yang sesuai untuk organisasi tertentu	Memberikan rekomendasi tepat disertai justifikasi kuat berdasarkan karakteristik organisasi	Memberikan rekomendasi dengan justifikasi cukup	Rekomendasi kurang tepat atau tanpa justifikasi	Tidak memberikan rekomendasi

Pertemuan 4: Sub-CPMK 2.1 – Kriptografi Simetris dan Asimetris (Bobot 2%)

Tugas: Analisis penerapan kriptografi dalam e-commerce, email, dan perbankan

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Pemahaman Konsep	Kemampuan menjelaskan perbedaan kriptografi simetris dan asimetris	Menjelaskan dengan sangat jelas perbedaan, kelebihan, kekurangan, dan contoh algoritma masing-masing	Menjelaskan dengan cukup jelas namun kurang detail	Penjelasan kurang jelas atau ada kesalahan konsep	Tidak memahami perbedaan
Analisis Skenario	Kemampuan menganalisis skenario penggunaan dalam aplikasi nyata	Menganalisis 3 skenario (e-commerce, email, perbankan) dengan tepat, menjelaskan algoritma yang digunakan dan alasannya	Menganalisis 2 skenario dengan cukup tepat	Menganalisis 1 skenario dengan sederhana	Tidak dapat menganalisis
Evaluasi Keamanan	Kemampuan mengevaluasi keamanan implementasi	Mengevaluasi kelebihan dan kelemahan implementasi kriptografi dalam setiap skenario disertai rekomendasi perbaikan	Mengevaluasi secara umum tanpa rekomendasi spesifik	Evaluasi dangkal atau tidak tepat	Tidak ada evaluasi

Pertemuan 5: Sub-CPMK 2.2 – Hash dan Digital Signature (Bobot 2%)

Tugas: Analisis penggunaan hash untuk verifikasi integritas dan digital signature pada dokumen elektronik

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Pemahaman Hash	Kemampuan menjelaskan fungsi hash dan aplikasinya	Menjelaskan sifat-sifat hash (one-way, collision resistance), contoh algoritma, dan aplikasi verifikasi integritas dengan sangat jelas	Menjelaskan dengan cukup baik namun kurang detail	Penjelasan kurang lengkap atau ada kesalahan	Tidak memahami konsep hash
Pemahaman Digital Signature	Kemampuan menjelaskan digital signature dan cara kerjanya	Menjelaskan proses pembuatan dan verifikasi digital signature, peran hash, dan contoh implementasi dengan sangat jelas	Menjelaskan dengan cukup baik	Penjelasan kurang lengkap	Tidak memahami digital signature
Analisis Kasus	Kemampuan menganalisis kasus penggunaan dalam dokumen elektronik	Menganalisis 2+ kasus (kontrak digital, dokumen pemerintah, software distribution) dengan detail dan tepat	Menganalisis 1 kasus dengan cukup baik	Analisis dangkal	Tidak ada analisis

Pertemuan 6: Sub-CPMK 2.3 – Infrastruktur Kunci Publik (PKI) (Bobot 2%)

Tugas: Analisis implementasi SSL/TLS pada website dan evaluasi sertifikat digital

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Pemahaman PKI	Kemampuan menjelaskan komponen PKI (CA, RA, sertifikat)	Menjelaskan dengan sangat jelas hierarki trust, peran masing-masing komponen, dan proses penerbitan sertifikat	Menjelaskan dengan cukup baik	Penjelasan kurang lengkap	Tidak memahami PKI
Analisis Sertifikat	Kemampuan menganalisis informasi sertifikat SSL pada website	Menganalisis minimal 3 website, mengidentifikasi issuer, masa berlaku, algoritma, dan mengevaluasi keamanannya	Menganalisis 2 website dengan cukup baik	Menganalisis 1 website dengan sederhana	Tidak dapat menganalisis
Evaluasi Keamanan	Kemampuan mengevaluasi keamanan implementasi SSL/TLS	Mengevaluasi potensi kerentanan (misal: sertifikat self-signed, usang, cipher lemah) dan memberikan rekomendasi perbaikan	Mengevaluasi secara umum tanpa rekomendasi	Evaluasi dangkal	Tidak ada evaluasi

Pertemuan 7: Sub-CPMK 3.1 – Analisis Risiko Keamanan (Bobot 2.5%)

Tugas: Melakukan analisis risiko untuk organisasi fiktif (UKM/rumah sakit) dan membuat matriks risiko

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Identifikasi Aset	Kemampuan mengidentifikasi aset informasi organisasi	Mengidentifikasi 10+ aset dengan klasifikasi nilai dan kepentingan yang tepat	Mengidentifikasi 7-9 aset dengan cukup lengkap	Mengidentifikasi 4-6 aset dengan penjelasan minimal	<4 aset atau tidak relevan
Penilaian Risiko	Ketepatan menilai likelihood dan impact	Menilai risiko dengan akurat menggunakan skala yang konsisten, disertai justifikasi kuat	Menilai dengan cukup akurat namun justifikasi kurang	Penilaian kurang konsisten atau tanpa justifikasi	Penilaian tidak akurat
Matriks Risiko	Kualitas visualisasi dan prioritas risiko	Matriks risiko sangat jelas, menunjukkan prioritas (tinggi, sedang, rendah) dengan tepat, dan dilengkapi analisis	Matriks cukup jelas dengan prioritas yang tepat	Matriks sederhana dengan beberapa elemen	Matriks tidak lengkap atau salah

Pertemuan 9: Sub-CPMK 3.2 – Perancangan Kontrol Keamanan (Bobot 2%)

Tugas: Merancang kontrol keamanan untuk mitigasi risiko yang telah diidentifikasi

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Relevansi Kontrol	Kesesuaian kontrol dengan risiko	Semua kontrol yang dirancang sangat relevan dan efektif untuk mitigasi risiko spesifik	Sebagian besar kontrol relevan	Beberapa kontrol kurang relevan	Kontrol tidak relevan
Kelengkapan Aspek	Cakupan kontrol administratif, teknis, dan fisik	Mencakup ketiga aspek dengan detail implementasi yang jelas	Mencakup dua aspek dengan cukup detail	Mencakup satu aspek dengan detail minimal	Tidak mencakup aspek yang diperlukan
Feasibility	Kemungkinan implementasi kontrol	Semua kontrol feasible dengan pertimbangan biaya, sumber daya, dan kompleksitas yang realistis	Sebagian besar kontrol feasible	Beberapa kontrol tidak feasible	Kontrol tidak feasible

Pertemuan 10: Sub-CPMK 3.3 – Penyusunan Kebijakan Keamanan (Bobot 2.5%)

Tugas: Menyusun kebijakan keamanan sederhana (Acceptable Use Policy atau Password Policy)

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Kelengkapan Struktur	Kesesuaian dengan template kebijakan	Kebijakan lengkap dengan: tujuan, ruang lingkup, definisi, kebijakan, sanksi, dan review	Memiliki sebagian besar elemen	Hanya memiliki beberapa elemen	Struktur tidak lengkap
Kejelasan Bahasa	Kejelasan dan ketepatan bahasa	Bahasa sangat jelas, tidak ambigu, konsisten, dan profesional	Bahasa cukup jelas dengan sedikit ambiguitas	Bahasa kurang jelas atau ambigu	Bahasa tidak jelas
Kesesuaian Standar	Mengacu pada standar keamanan	Kebijakan sangat sesuai dengan ISO 27001 atau NIST, mengacu pada klausul spesifik	Cukup sesuai dengan prinsip umum	Kurang sesuai	Tidak sesuai

Pertemuan 11: Sub-CPMK 4.1 – Analisis Keamanan Jaringan (Firewall, IDS/IPS) (Bobot 2%)

Tugas: Menganalisis konfigurasi firewall pada skenario jaringan tertentu

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Pemahaman Firewall	Kemampuan menjelaskan fungsi dan jenis firewall	Menjelaskan dengan sangat jelas packet filtering, stateful inspection, application firewall, dan contoh implementasi	Menjelaskan dengan cukup baik	Penjelasan kurang lengkap	Tidak memahami
Analisis Konfigurasi	Kemampuan menganalisis aturan firewall	Menganalisis aturan firewall (allow/deny) pada skenario, mengidentifikasi kelemahan, dan merekomendasikan perbaikan	Menganalisis dengan cukup baik namun kurang rekomendasi	Analisis dangkal	Tidak dapat menganalisis
Pemahaman IDS/IPS	Kemampuan menjelaskan perbedaan IDS dan IPS	Menjelaskan dengan sangat jelas deteksi vs pencegahan, signature-based vs anomaly-based	Menjelaskan dengan cukup baik	Penjelasan kurang	Tidak memahami

Pertemuan 12: Sub-CPMK 4.1 – Lanjutan Analisis Keamanan Jaringan (Arsitektur Jaringan Aman) (Bobot 2%)

Tugas: Menganalisis desain arsitektur jaringan organisasi

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Analisis Arsitektur	Kemampuan menganalisis kelemahan arsitektur	Mengidentifikasi 5+ kelemahan arsitektur (misal: kurang segmentasi, DMZ tidak tepat, single point of failure) dengan analisis mendalam	Mengidentifikasi 3-4 kelemahan dengan cukup baik	Mengidentifikasi 1-2 kelemahan	Tidak ada identifikasi
Pemahaman Zero Trust	Kemampuan menjelaskan konsep Zero Trust	Menjelaskan dengan sangat jelas prinsip "never trust, always verify", micro-segmentation, dan implementasinya	Menjelaskan dengan cukup baik	Penjelasan kurang	Tidak memahami
Rekomendasi Perbaikan	Kualitas rekomendasi perbaikan	Memberikan rekomendasi spesifik, detail, dan feasible untuk setiap kelemahan	Rekomendasi cukup spesifik	Rekomendasi umum	Tidak ada rekomendasi

Pertemuan 13: Sub-CPMK 4.2 – Kerentanan Keamanan Aplikasi (OWASP Top 10) (Bobot 2%)

Tugas: Menganalisis kerentanan pada aplikasi web fiktif berdasarkan OWASP Top 10

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Identifikasi Kerentanan	Kemampuan mengidentifikasi kerentanan OWASP	Mengidentifikasi 5+ kerentanan dari OWASP Top 10 dengan deskripsi tepat dan contoh skenario	Mengidentifikasi 3-4 kerentanan dengan cukup baik	Mengidentifikasi 1-2 kerentanan	Tidak dapat mengidentifikasi
Pemahaman Dampak	Kemampuan menjelaskan dampak kerentanan	Menjelaskan dampak terhadap kerahasiaan, integritas, ketersediaan, serta potensi eksploitasi dengan sangat jelas	Menjelaskan dampak secara umum	Penjelasan dangkal	Tidak ada penjelasan
Rekomendasi Perbaikan	Kualitas rekomendasi perbaikan	Memberikan rekomendasi perbaikan yang spesifik (misal: input validation, parameterized queries) dan sesuai standar secure coding	Rekomendasi cukup spesifik	Rekomendasi umum	Tidak ada rekomendasi

Pertemuan 14: Sub-CPMK 4.3 – Aspek Hukum dan Etika (UU ITE, UU PDP) (Bobot 2%)

Tugas: Analisis kasus pelanggaran UU ITE dan cyber crime

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Pemahaman Regulasi	Kemampuan menjelaskan UU ITE dan UU PDP	Menjelaskan dengan sangat jelas pasal-pasal terkait cyber crime, perlindungan data pribadi, dan sanksi	Menjelaskan dengan cukup baik	Penjelasan kurang lengkap	Tidak memahami
Analisis Kasus Hukum	Kemampuan menganalisis kasus hukum	Menganalisis 2+ kasus dengan mengidentifikasi pasal yang dilanggar, modus, dan putusan (jika ada)	Menganalisis 1 kasus dengan cukup baik	Analisis dangkal	Tidak ada analisis
Etika Profesional	Kemampuan mengevaluasi dilema etika	Mengevaluasi dilema etika (whistleblowing, ethical hacking) dengan argumen kuat dan perspektif multiple	Mengevaluasi dengan cukup baik	Evaluasi sederhana	Tidak ada evaluasi

Pertemuan 15: Sub-CPMK 4.3 – Lanjutan Aspek Hukum dan Kepatuhan (Bobot 2%)

Tugas: Presentasi kelompok tentang tren keamanan terkini dan implikasi kepatuhan

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Kualitas Presentasi	Kejelasan, sistematika, dan komunikasi	Presentasi sangat jelas, sistematis, komunikatif, menggunakan media yang menarik, dan waktu tepat	Presentasi cukup jelas dan sistematis	Presentasi kurang sistematis atau sulit dipahami	Presentasi tidak terstruktur
Kedalaman Analisis Tren	Kemampuan menganalisis tren keamanan (AI security, IoT, cloud)	Analisis mendalam tentang tren, dampak, tantangan, dan peluang, disertai contoh nyata	Analisis cukup baik dengan beberapa contoh	Analisis dangkal	Tidak ada analisis
Implikasi Kepatuhan	Kemampuan menjelaskan implikasi kepatuhan terhadap regulasi	Menjelaskan dengan sangat jelas bagaimana tren mempengaruhi kepatuhan terhadap UU/standar, dan rekomendasi adaptasi	Menjelaskan dengan cukup baik	Penjelasan kurang	Tidak ada penjelasan

C. RUBRIK PARTISIPASI (Bobot 10%)

Penilaian partisipasi dilakukan setiap pertemuan dan diakumulasi pada akhir semester.

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Keaktifan Bertanya/Menjawab	40%	Aktif bertanya/menjawab dengan pertanyaan mendalam minimal 2x per pertemuan	Aktif 1x per pertemuan	Jarang bertanya/menjawab (1-2x selama semester)	Tidak pernah berpartisipasi
Kualitas Kontribusi	30%	Kontribusi konstruktif, mengaitkan konsep, memperkaya diskusi, dan relevan	Kontribusi relevan dan tepat	Kontribusi sederhana, mengulang pendapat	Kontribusi tidak relevan atau mengganggu
Kehadiran dan Ketepatan Waktu	30%	Hadir tepat waktu di semua 16 pertemuan	Hadir tepat waktu di ≥14 pertemuan	Hadir di 12-13 pertemuan, beberapa terlambat	Hadir <12 pertemuan

D. RUBRIK UJIAN TENGAH SEMESTER (UTS) – Bobot 30%

UTS terdiri dari soal teori (40%) dan studi kasus (60%). Total nilai UTS = (Nilai teori × 40%) + (Nilai studi kasus × 60%).

Komponen Teori (40% dari nilai UTS)

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Ketepatan Jawaban	50%	Semua jawaban tepat dengan penjelasan akurat dan lengkap	Sebagian besar jawaban tepat dengan sedikit kesalahan	Beberapa jawaban tepat, beberapa salah	Banyak jawaban salah atau tidak dijawab
Pemahaman Konsep	50%	Menunjukkan pemahaman mendalam, mampu mengaitkan antar konsep	Menunjukkan pemahaman cukup baik	Pemahaman dasar, kurang mengaitkan	Tidak memahami konsep

Komponen Studi Kasus (60% dari nilai UTS)

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Analisis Kasus	40%	Analisis sangat tepat, komprehensif, mengidentifikasi semua isu kunci	Analisis tepat, mengidentifikasi sebagian besar isu	Analisis cukup tepat, beberapa isu terlewat	Analisis dangkal atau salah
Penerapan Konsep	30%	Menerapkan konsep yang relevan dengan sangat tepat dan kreatif	Menerapkan konsep dengan tepat	Kurang tepat dalam penerapan	Tidak menerapkan konsep
Solusi dan Rekomendasi	30%	Memberikan solusi yang spesifik, feasible, dan inovatif	Solusi cukup spesifik dan feasible	Solusi umum dan kurang feasible	Solusi tidak relevan

E. RUBRIK UJIAN AKHIR SEMESTER (UAS) – Bobot 30%

UAS terdiri dari soal teori (40%) dan studi kasus (60%). Total nilai UAS = (Nilai teori × 40%) + (Nilai studi kasus × 60%).

Komponen Teori (40% dari nilai UAS)

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Ketepatan Jawaban	50%	Semua jawaban tepat dengan penjelasan akurat dan lengkap	Sebagian besar jawaban tepat	Beberapa jawaban tepat	Banyak jawaban salah
Pemahaman Konsep	50%	Menunjukkan pemahaman mendalam, mampu mengaitkan antar konsep	Pemahaman cukup baik	Pemahaman dasar	Tidak memahami

Komponen Studi Kasus (60% dari nilai UAS)

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Analisis Kasus	40%	Analisis sangat tepat, komprehensif, mengidentifikasi semua isu kunci	Analisis tepat, mengidentifikasi sebagian besar isu	Analisis cukup tepat, beberapa isu terlewat	Analisis dangkal atau salah
Penerapan Konsep	30%	Menerapkan konsep dengan sangat tepat dan kreatif	Menerapkan konsep dengan tepat	Kurang tepat dalam penerapan	Tidak menerapkan konsep
Solusi dan Rekomendasi	30%	Solusi spesifik, feasible, inovatif, dan mempertimbangkan aspek hukum/etika	Solusi cukup spesifik dan feasible	Solusi umum	Solusi tidak relevan

F. REKAPITULASI PENILAIAN

Komponen	Bobot	Nilai Maksimal
Tugas Pertemuan 1	2%	100
Tugas Pertemuan 2	2%	100
Tugas Pertemuan 3	2.5%	100
Tugas Pertemuan 4	2%	100
Tugas Pertemuan 5	2%	100
Tugas Pertemuan 6	2%	100
Tugas Pertemuan 7	2.5%	100
Tugas Pertemuan 9	2%	100
Tugas Pertemuan 10	2.5%	100
Tugas Pertemuan 11	2%	100
Tugas Pertemuan 12	2%	100
Tugas Pertemuan 13	2%	100
Tugas Pertemuan 14	2%	100
Tugas Pertemuan 15	2%	100

Komponen	Bobot	Nilai Maksimal
Subtotal Tugas	**30%**	
Partisipasi	10%	100
UTS	30%	100
UAS	30%	100
Total	**100%**	

Nilai Akhir = (Rata-rata nilai tugas × 30%) + (Nilai partisipasi × 10%) + (Nilai UTS × 30%) + (Nilai UAS × 30%)

G. KONVERSI NILAI AKHIR KE HURUF

Rentang Nilai	Nilai Huruf	Indeks Prestasi
85.00 – 100.00	A	4.00
80.00 – 84.99	A-	3.75
75.00 – 79.99	B+	3.50
70.00 – 74.99	B	3.00
65.00 – 69.99	B-	2.75
60.00 – 64.99	C+	2.50

Rentang Nilai	Nilai Huruf	Indeks Prestasi
55.00 – 59.99	C	2.00
50.00 – 54.99	D	1.00
0.00 – 49.99	E	0.00

Ditetapkan di: Padang
Tanggal: 23 Februari 2026
Dosen Pengampu,

Ir. H. A. Mooduto, M.Kom.
NIP. 196605101994031003

RUBRIK PENILAIAN RENCANA PEMBELAJARAN SEMESTER (RPS)
MATA KULIAH KEAMANAN SISTEM INFORMASI (ISY3210) – 1 SKS Praktik
Program Studi D3-Manajemen Informatika Politeknik Negeri Padang

---

A. RUBRIK UMUM TUGAS PRAKTIKUM PER PERTEMUAN

Rubrik ini digunakan sebagai acuan penilaian untuk setiap tugas praktikum pada pertemuan 1-7 dan 9-15. Setiap tugas memiliki bobot 2% atau 2.5% dengan rentang nilai 0-100. Nilai akhir tugas = (Skor total / 100) × Bobot tugas.

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Keberhasilan Praktik	50%	Semua langkah praktikum berhasil dijalankan dengan sempurna, tidak ada error, output sesuai dengan yang diharapkan, dan dapat didemonstrasikan	Sebagian besar langkah berhasil (≥80%), terdapat error minor yang dapat diatasi, output sebagian besar sesuai	Beberapa langkah gagal (50-79%), error signifikan namun masih ada output yang dihasilkan	Sebagian besar langkah gagal (<50%) atau tidak dapat menyelesaikan praktikum
Pemahaman Prosedur	25%	Menjelaskan setiap langkah dengan tepat, memahami tujuan dan konsep di balik setiap perintah, mampu menjawab pertanyaan terkait dengan baik	Menjelaskan sebagian besar langkah dengan cukup tepat, memahami tujuan umum, mampu menjawab sebagian pertanyaan	Menjelaskan beberapa langkah dengan kurang tepat, pemahaman terbatas, sulit menjawab pertanyaan	Tidak dapat menjelaskan prosedur, tidak memahami tujuan praktikum
Kualitas Laporan	25%	Laporan praktikum sangat lengkap (pendahuluan, langkah-langkah, screenshot, analisis, kesimpulan), sistematis, bahasa jelas, dan analisis mendalam	Laporan cukup lengkap, sistematis, bahasa cukup jelas, analisis cukup	Laporan kurang lengkap, kurang sistematis, analisis dangkal	Laporan tidak lengkap, tidak sistematis, atau tidak ada laporan

---

B. RUBRIK KHUSUS PER PERTEMUAN

Pertemuan 1: Sub-CPMK 1.1 – Enkripsi/Dekripsi dengan OpenSSL (Bobot 2%)

Tugas: Melakukan enkripsi dan dekripsi file menggunakan OpenSSL (AES dan RSA)

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Keberhasilan Enkripsi AES	Mampu mengenkripsi dan mendekripsi file dengan AES	Berhasil melakukan enkripsi dan dekripsi dengan AES-256, file hasil dekripsi identik dengan file asli	Berhasil enkripsi/dekripsi dengan AES, namun ada sedikit masalah (misal: parameter kurang tepat)	Hanya berhasil enkripsi atau dekripsi saja	Gagal melakukan enkripsi/dekripsi
Keberhasilan RSA	Mampu membuat key pair RSA dan melakukan enkripsi/dekripsi	Berhasil membuat key pair, enkripsi dengan public key, dekripsi dengan private key, semua berjalan sempurna	Berhasil membuat key pair, namun enkripsi/dekripsi kurang sempurna	Hanya berhasil membuat key pair	Gagal total
Dokumentasi	Kelengkapan laporan praktikum	Laporan lengkap dengan screenshot setiap langkah, penjelasan, dan analisis perbedaan AES vs RSA	Laporan cukup lengkap, ada screenshot	Laporan kurang lengkap	Tidak ada laporan

Pertemuan 2: Sub-CPMK 1.2 – Digital Signature dengan OpenSSL (Bobot 2%)

Tugas: Membuat dan memverifikasi digital signature, menghitung hash

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Perhitungan Hash	Menghitung hash file dengan SHA-256	Berhasil menghitung hash, hasil konsisten, mampu menjelaskan fungsi hash	Berhasil menghitung hash, namun kurang memahami konsep	Hash dihitung tapi tidak konsisten	Gagal menghitung hash
Pembuatan Signature	Membuat digital signature dengan kunci privat	Berhasil membuat signature, file signature terbentuk	Signature dibuat namun ada kesalahan parameter	Signature tidak valid	Gagal membuat signature
Verifikasi Signature	Memverifikasi signature dengan kunci publik	Berhasil verifikasi (status OK), mampu menjelaskan proses	Verifikasi berhasil namun kurang paham	Verifikasi gagal	Tidak melakukan verifikasi
Laporan	Kualitas laporan	Laporan lengkap, ada screenshot, analisis, dan kesimpulan	Laporan cukup	Laporan kurang	Tidak ada

Pertemuan 3: Sub-CPMK 1.3 – Hash untuk Verifikasi Integritas (Bobot 2.5%)

Tugas: Menghitung hash sebelum dan sesudah modifikasi file, analisis perubahan

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Perhitungan Hash	Menghitung hash file asli dan setelah modifikasi	Berhasil menghitung hash kedua file dengan tepat, mencatat nilai hash	Hash dihitung dengan benar	Hash dihitung namun kurang teliti	Gagal
Deteksi Perubahan	Membandingkan hash dan menyimpulkan	Menyimpulkan dengan tepat bahwa file berubah karena hash berbeda, menjelaskan aplikasi verifikasi integritas	Menyimpulkan dengan benar	Kesimpulan kurang tepat	Tidak ada kesimpulan
Eksperimen	Melakukan modifikasi file (misal: ubah 1 karakter) dan uji coba	Melakukan minimal 3 skenario modifikasi, analisis perbedaan hash	2 skenario	1 skenario	Tidak ada
Laporan	Kelengkapan	Laporan sangat lengkap, analisis mendalam	Cukup	Kurang	Tidak ada

Pertemuan 4: Sub-CPMK 2.1 – Identifikasi Aset dan Analisis Risiko (Bobot 2%)

Tugas: Identifikasi aset organisasi fiktif, penilaian risiko, matriks risiko

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Identifikasi Aset	Jumlah dan kelengkapan aset	Mengidentifikasi ≥10 aset dengan kategori (hardware, software, data, manusia) dan nilai aset	7-9 aset	4-6 aset	<4 aset
Penilaian Risiko	Penilaian likelihood dan impact	Menilai setiap aset dengan skala konsisten (1-5), memberikan justifikasi	Penilaian cukup konsisten	Penilaian tidak konsisten	Tidak ada penilaian
Matriks Risiko	Visualisasi dan prioritas	Matriks risiko jelas, menunjukkan prioritas (tinggi, sedang, rendah), dilengkapi analisis	Matriks cukup jelas	Matriks sederhana	Tidak ada matriks
Laporan	Kelengkapan	Laporan lengkap, terstruktur	Cukup	Kurang	Tidak ada

Pertemuan 5: Sub-CPMK 2.2 – Menyusun Kebijakan Keamanan (Bobot 2%)

Tugas: Menyusun Acceptable Use Policy (AUP) dan Password Policy

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Kelengkapan Struktur	Memiliki semua elemen kebijakan (tujuan, ruang lingkup, definisi, kebijakan, sanksi, review)	Kedua kebijakan memiliki struktur lengkap dan profesional	Satu kebijakan lengkap, satu kurang	Kedua kurang lengkap	Tidak ada struktur
Kejelasan Bahasa	Bahasa jelas, tidak ambigu, dan mudah dipahami	Bahasa sangat jelas, formal, dan konsisten	Bahasa cukup jelas	Bahasa kurang jelas	Bahasa tidak jelas
Kesesuaian Standar	Mengacu pada standar (ISO 27001 atau NIST)	Kebijakan sesuai dengan rekomendasi standar, ada referensi	Cukup sesuai	Kurang sesuai	Tidak sesuai
Kreativitas	Penyesuaian dengan konteks organisasi	Sangat kontekstual dan relevan dengan organisasi fiktif	Cukup kontekstual	Kurang kontekstual	Tidak relevan

Pertemuan 6: Sub-CPMK 3.1 – Konfigurasi Firewall iptables (Bobot 2%)

Tugas: Mengkonfigurasi aturan iptables untuk memblokir port, mengatur forwarding

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Keberhasilan Konfigurasi	Aturan dapat dijalankan dan bekerja	Semua aturan berhasil, pengujian menunjukkan port yang diblokir tidak bisa diakses, port lain tetap bisa	Sebagian besar aturan berhasil (≥80%)	Beberapa aturan gagal	Gagal total
Pemahaman Aturan	Menjelaskan setiap aturan	Menjelaskan arti setiap baris perintah dengan tepat	Menjelaskan sebagian	Kurang jelas	Tidak bisa menjelaskan
Pengujian	Melakukan pengujian dengan tools (ping, telnet, nc)	Melakukan pengujian komprehensif, mendokumentasikan hasil	Pengujian cukup	Pengujian minimal	Tidak ada pengujian
Laporan	Kelengkapan	Laporan lengkap dengan screenshot konfigurasi dan hasil uji	Cukup	Kurang	Tidak ada

Pertemuan 7: Sub-CPMK 3.2 – Instalasi dan Konfigurasi Snort IDS (Bobot 2.5%)

Tugas: Instal Snort, konfigurasi rules, deteksi serangan

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Instalasi	Snort terinstal dengan benar	Instalasi sukses, Snort dapat dijalankan	Instalasi sukses namun ada warning	Instalasi bermasalah	Gagal instalasi
Konfigurasi Rules	Membuat rule sederhana (misal: deteksi ping, port scan)	Rule berhasil dibuat dan aktif, Snort menghasilkan alert saat serangan	Rule aktif namun alert tidak muncul	Rule tidak aktif	Tidak membuat rule
Deteksi Serangan	Melakukan serangan uji (ping flood, nmap)	Serangan terdeteksi dengan alert yang sesuai, log tercatat	Terdeteksi sebagian	Tidak terdeteksi	Tidak ada pengujian
Laporan	Kelengkapan	Laporan lengkap, ada screenshot alert	Cukup	Kurang	Tidak ada

Pertemuan 9: Sub-CPMK 3.3 – Konfigurasi VPN OpenVPN (Bobot 2%)

Tugas: Instalasi OpenVPN server, konfigurasi client, koneksi

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Instalasi Server	OpenVPN server terinstal dan konfigurasi dasar	Server berjalan dengan baik, sertifikat CA dibuat	Server berjalan namun ada masalah kecil	Server tidak berjalan	Gagal
Konfigurasi Client	Membuat sertifikat client dan konfigurasi	Client berhasil terkoneksi ke server, mendapat IP VPN	Koneksi berhasil namun lambat	Koneksi gagal	Tidak ada
Enkripsi	Memastikan traffic terenkripsi (dengan Wireshark)	Traffic VPN terlihat terenkripsi, mampu menjelaskan	Terenkripsi namun tidak dianalisis	Tidak dicek	Tidak ada
Laporan	Kelengkapan	Laporan lengkap, ada screenshot koneksi	Cukup	Kurang	Tidak ada

Pertemuan 10: Sub-CPMK 3.4 – Analisis Jaringan dengan Wireshark dan Nmap (Bobot 2.5%)

Tugas: Menggunakan Wireshark untuk analisis traffic, Nmap untuk scanning

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Wireshark	Mampu menangkap traffic, menganalisis packet (HTTP, TCP handshake)	Menangkap traffic, mengidentifikasi dengan tepat jenis packet, menjelaskan isi	Mampu menangkap dan identifikasi sebagian	Kurang tepat	Tidak bisa
Nmap	Melakukan port scanning, service detection	Berhasil scan, mengidentifikasi port terbuka dan layanan, menjelaskan hasil	Scan berhasil, identifikasi sebagian	Scan gagal	Tidak melakukan
Integrasi	Menghubungkan hasil Nmap dan Wireshark	Menganalisis korelasi antara port terbuka dan traffic yang ditangkap	Ada korelasi sederhana	Tidak ada korelasi	-
Laporan	Kelengkapan	Laporan lengkap, analisis mendalam	Cukup	Kurang	Tidak ada

Pertemuan 11: Sub-CPMK 4.1 – Vulnerability Scanning dengan Nessus (Bobot 2%)

Tugas: Instalasi Nessus, scan jaringan, analisis laporan

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Instalasi	Nessus terinstal dan dapat diakses	Instalasi sukses, dapat login	Instalasi sukses namun ada kendala akses	Instalasi gagal	-
Scanning	Melakukan basic network scan	Scan berhasil, mendapatkan hasil kerentanan	Scan berhasil namun hasil kurang lengkap	Scan gagal	Tidak melakukan
Analisis Hasil	Membaca laporan, memahami tingkat keparahan	Mampu menjelaskan temuan, tingkat risiko, dan dampak	Menjelaskan sebagian	Kurang memahami	Tidak ada analisis
Laporan	Kelengkapan	Laporan lengkap, mencakup rekomendasi perbaikan	Cukup	Kurang	Tidak ada

Pertemuan 12: Sub-CPMK 4.1 – Vulnerability Scanning dengan OWASP ZAP (Bobot 2%)

Tugas: Menggunakan OWASP ZAP untuk scan aplikasi web

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Konfigurasi	Mengatur OWASP ZAP, spidering	Berhasil melakukan spidering pada target	Spidering berjalan	Gagal	-
Active Scan	Melakukan active scan	Scan berhasil, mendapatkan alert kerentanan	Scan berhasil namun alert sedikit	Scan gagal	-
Analisis	Menganalisis alert yang muncul	Mampu menjelaskan setiap alert (SQLi, XSS, dll) dan dampaknya	Menjelaskan sebagian	Tidak paham	-
Laporan	Kelengkapan	Laporan lengkap, ada screenshot, rekomendasi	Cukup	Kurang	Tidak ada

Pertemuan 13: Sub-CPMK 4.2 – Identifikasi Kerentanan OWASP Top 10 (Bobot 2%)

Tugas: Menguji aplikasi web rentan (DVWA) dan mengidentifikasi SQLi, XSS

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Eksploitasi SQLi	Berhasil melakukan SQL injection	Berhasil mengekstrak data dari database, menunjukkan bukti	Berhasil namun data terbatas	Gagal	-
Eksploitasi XSS	Berhasil melakukan reflected/stored XSS	Berhasil memicu pop-up alert atau mencuri cookie	Berhasil namun sederhana	Gagal	-
Dokumentasi	Mencatat langkah-langkah	Mendokumentasikan dengan jelas payload dan hasil	Cukup	Kurang	Tidak ada
Laporan	Kelengkapan	Laporan lengkap, analisis dampak	Cukup	Kurang	Tidak ada

Pertemuan 14: Sub-CPMK 4.3 – Membuat Laporan Hasil Pengujian (Bobot 2%)

Tugas: Menyusun laporan dari hasil scanning dan identifikasi kerentanan

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Struktur Laporan	Memiliki pendahuluan, metodologi, temuan, analisis, rekomendasi	Struktur lengkap dan profesional	Cukup lengkap	Kurang lengkap	Tidak terstruktur
Kualitas Temuan	Menjelaskan temuan dengan detail	Menjelaskan setiap temuan (jenis, tingkat risiko, lokasi) dengan jelas	Cukup jelas	Kurang jelas	Tidak ada
Rekomendasi	Memberikan rekomendasi perbaikan yang spesifik	Rekomendasi spesifik, feasible, dan prioritas	Cukup spesifik	Rekomendasi umum	Tidak ada
Bahasa	Bahasa formal, jelas, dan bebas typo	Sangat baik	Cukup	Kurang	Buruk

Pertemuan 15: Proyek Kelompok – Simulasi Keamanan Terintegrasi (Bobot 2%)

Tugas: Proyek kelompok mengintegrasikan semua praktikum, presentasi

Kriteria	Indikator Penilaian	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Kualitas Proyek	Kelengkapan dan kedalaman	Proyek mencakup analisis risiko, konfigurasi keamanan, pengujian, dan laporan, semuanya terintegrasi dengan baik	Mencakup sebagian besar	Hanya beberapa bagian	Tidak lengkap
Kerja Tim	Pembagian tugas dan kerjasama	Semua anggota berkontribusi aktif, kolaborasi baik	Sebagian besar aktif	Hanya beberapa	Tidak ada kerjasama
Presentasi	Kejelasan, visual, komunikasi	Presentasi sangat jelas, menarik, menjawab pertanyaan dengan baik	Cukup jelas	Kurang jelas	Tidak presentasi
Laporan Proyek	Kelengkapan laporan	Laporan proyek lengkap, sistematis	Cukup	Kurang	Tidak ada

C. RUBRIK PARTISIPASI (Bobot 10%)

Penilaian partisipasi dilakukan setiap pertemuan dan diakumulasi pada akhir semester.

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Keaktifan dalam Praktikum	40%	Selalu aktif bertanya, mencoba hal baru, membantu teman, inisiatif tinggi	Cukup aktif, sesekali bertanya	Jarang aktif, hanya mengikuti instruksi	Pasif, tidak berkontribusi
Kedisiplinan	30%	Hadir tepat waktu di setiap pertemuan (100%), menyelesaikan tugas tepat waktu	Hadir tepat waktu ≥14 pertemuan, tugas sebagian besar tepat waktu	Sering terlambat atau tidak hadir (≥3 kali)	Sering tidak hadir (>3 kali)
Kerjasama Kelompok	30%	Bekerja sama dengan baik, komunikatif, menghargai pendapat teman	Cukup baik	Kurang kooperatif	Tidak mau bekerja sama

---

D. RUBRIK UJIAN TENGAH SEMESTER (UTS) PRAKTIKUM – Bobot 30%

UTS berupa ujian praktik individu yang mencakup materi pertemuan 1-7. Mahasiswa diberikan serangkaian tugas yang harus diselesaikan dalam waktu 170 menit.

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Ketepatan Hasil	50%	Semua tugas (enkripsi, signature, firewall, Snort) diselesaikan dengan hasil tepat dan sempurna	Sebagian besar tugas selesai dengan hasil tepat (≥80%)	Beberapa tugas selesai (50-79%) dengan hasil kurang tepat	<50% tugas selesai atau hasil salah
Efisiensi Waktu	25%	Selesai sebelum waktu yang ditentukan, langkah-langkah efisien	Selesai tepat waktu	Melebihi waktu tetapi masih selesai	Tidak selesai
Kemandirian	25%	Mengerjakan sendiri tanpa bantuan, tidak bertanya	Cukup mandiri, sesekali bertanya	Sering bertanya atau melihat pekerjaan teman	Bergantung penuh pada bantuan

---

E. RUBRIK UJIAN AKHIR SEMESTER (UAS) PRAKTIKUM – Bobot 30%

UAS berupa ujian praktik individu yang mencakup materi pertemuan 9-15 (VPN, Wireshark, Nmap, scanning, laporan).

Kriteria	Bobot	Sangat Baik (86-100)	Baik (71-85)	Cukup (56-70)	Kurang (<56)
Ketepatan Hasil	50%	Semua tugas (VPN koneksi, analisis Wireshark, scanning, laporan) selesai dengan hasil tepat	Sebagian besar selesai tepat	Beberapa selesai	Sebagian besar gagal
Kualitas Laporan	25%	Laporan ujian sangat lengkap, analisis mendalam, rekomendasi jelas	Laporan cukup	Laporan kurang	Tidak ada laporan
Kemandirian	25%	Mengerjakan sendiri, mampu menjelaskan langkah	Cukup mandiri	Kurang mandiri	Tidak mandiri

---

F. REKAPITULASI PENILAIAN

Komponen	Bobot	Nilai Maksimal
Tugas Pertemuan 1	2%	100
Tugas Pertemuan 2	2%	100
Tugas Pertemuan 3	2.5%	100
Tugas Pertemuan 4	2%	100
Tugas Pertemuan 5	2%	100
Tugas Pertemuan 6	2%	100
Tugas Pertemuan 7	2.5%	100

Komponen	Bobot	Nilai Maksimal
Tugas Pertemuan 9	2%	100
Tugas Pertemuan 10	2.5%	100
Tugas Pertemuan 11	2%	100
Tugas Pertemuan 12	2%	100
Tugas Pertemuan 13	2%	100
Tugas Pertemuan 14	2%	100
Tugas Pertemuan 15	2%	100
Subtotal Tugas	**30%**	
Partisipasi	10%	100
UTS	30%	100
UAS	30%	100
Total	**100%**	

Nilai Akhir = (Rata-rata nilai tugas × 30%) + (Nilai partisipasi × 10%) + (Nilai UTS × 30%) + (Nilai UAS × 30%)

G. KONVERSI NILAI AKHIR KE HURUF

Rentang Nilai	Nilai Huruf	Indeks Prestasi
85.00 – 100.00	A	4.00
80.00 – 84.99	A-	3.75
75.00 – 79.99	B+	3.50
70.00 – 74.99	B	3.00
65.00 – 69.99	B-	2.75
60.00 – 64.99	C+	2.50
55.00 – 59.99	C	2.00
50.00 – 54.99	D	1.00
0.00 – 49.99	E	0.00

Ditetapkan di: Padang
Tanggal: 23 Februari 2026
A/n Dosen Pengampu,

Ir. H. A. Mooduto
NIP. 196605101994031003