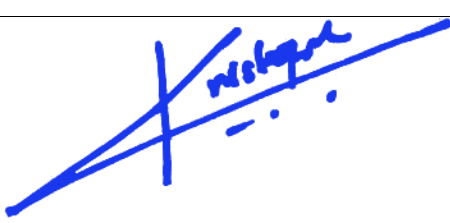
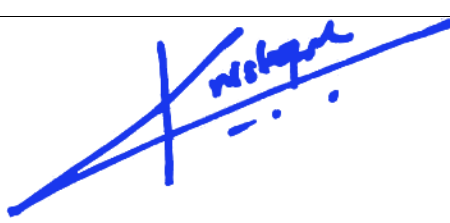


	UNIVERSITAS NEGERI MANADO								
	FAKULTAS TEKNIK								
	PROGRAM STUDI TEKNIK INFORMATIKA								
RENCANA PEMBELAJARAN SEMESTER (RPS)									
Nama Mata Kuliah	Kode	Rumpun MK	Bobot			Semester	Tahun Ajaran		
Cyber Security	5652042	Sistem Terdistribusi	T = 1	P = 1			Ganjil 2025/2026		
Otorisasi/Pengesahan	Pengembang RPS		Koordinator MK			Koordinator Prodi			
	Tim Pengembang RPS Prodi TI		 Sonyd Campvid Kumajas			 Kristofel Santa, S.ST, M.MT			
Capaian Pembelajaran Mata Kuliah	Capaian Pembelajaran Lulusan Program Studi (CPL Prodi) yang Dibebankan pada Mata Kuliah								
	CPL-1	Mampu menerapkan prinsip dasar ilmu komputer dalam menyelesaikan masalah teknis.							
	CPL-2	Mampu menganalisis dan mengembangkan sistem berbasis komputer secara profesional.							
	CPL-3	Mampu berkomunikasi secara efektif dalam tim multidisiplin.							
	CPL-4	Menunjukkan sikap profesional, etis, dan bertanggung jawab dalam praktek keilmuan.							
	CPL-5	Mampu mengikuti perkembangan teknologi informasi secara berkelanjutan.							
	Capaian Pembelajaran Mata Kuliah (CPMK)								
	CPMK-1	Memahami prinsip dasar keamanan siber (Cyber Security).							
	CPMK-2	Menganalisis ancaman dan kerentanan sistem informasi.							
	CPMK-3	Menerapkan teknik dasar pengamanan data dan jaringan.							
	CPMK-4	Mengembangkan kebijakan keamanan informasi yang sesuai standar industri.							
	CPMK-5	Mengintegrasikan pendekatan keamanan dalam pengembangan sistem berbasis proyek.							
	Kemampuan Akhir Tiap Tahapan Belajar (Sub-CPMK)								
	Sub-CPMK-1	Menjelaskan konsep dasar dan pentingnya keamanan siber.							
	Sub-CPMK-2	Mengidentifikasi jenis-jenis ancaman dan kerentanan sistem informasi.							
	Sub-CPMK-3	Menganalisis kasus serangan siber dan dampaknya.							
	Sub-CPMK-4	Menerapkan teknik kriptografi dasar dalam pengamanan data.							
	Sub-CPMK-5	Mendesain pengamanan jaringan dan sistem informasi sederhana.							
	Sub-CPMK-6	Mengembangkan dokumen kebijakan keamanan informasi.							
	Sub-CPMK-7	Mengimplementasikan prinsip keamanan dalam pengembangan sistem berbasis proyek.							
	Korelasi CPMK terhadap Sub-CPMK								
		Sub-CPMK-1	Sub-CPMK-2	Sub-CPMK-3	Sub-CPMK-4	Sub-CPMK-5	Sub-CPMK-6	Sub-CPMK-7	
	CPMK-1	√	√						
	CPMK-2		√	√					
	CPMK-3				√	√			
	CPMK-4						√		
	CPMK-5							√	
Deskripsi Singkat Mata Kuliah	Mata kuliah ini membahas prinsip-prinsip keamanan informasi dan keamanan jaringan. Mahasiswa akan mempelajari konsep dasar, jenis ancaman, teknik mitigasi, serta kebijakan keamanan informasi. Selain teori, mahasiswa juga dilatih untuk mampu mengembangkan solusi keamanan berbasis proyek dan studi kasus nyata.								

Bahan Kajian Materi Pembelajaran	Pengantar Cyber Security: Definisi, urgensi, ruang lingkup
	Prinsip dasar keamanan informasi: CIA Triad (Confidentiality, Integrity, Availability)
	Jenis-jenis ancaman: malware, phishing, ransomware, DDoS, insider threat
	Kerentanan sistem dan teknik eksploitasi
	Analisis insiden keamanan siber dan penanganan awal
	Dampak serangan siber terhadap organisasi dan individu
	Teknik dasar kriptografi: simetris, asimetris, hash, digital signature
	Desain pengamanan jaringan: firewall, IDS/IPS, segmentasi jaringan
	Implementasi firewall, honeypot, dan pengujian penetrasi dasar
	Perumusan kebijakan keamanan: kebijakan user, password, backup, akses
	Evaluasi dan review kebijakan keamanan
	Integrasi keamanan dalam pengembangan sistem berbasis proyek
	Implementasi keamanan pada proyek sistem nyata
	Presentasi hasil proyek keamanan
Bahan Pustaka	Stallings, William. (2020). Cryptography and Network Security. Pearson.
	Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security. Cengage Learning.
	Choraś, Michal. (2020). Cybersecurity Essentials. Springer.
	Goodrich, M. T., & Tamassia, R. (2014). Introduction to Computer Security. Pearson.
	Anderson, Ross. (2020). Security Engineering. Wiley.
Dosen Pengampu	Sondy Campvid Kumajas
Mata Kuliah Prasyarat	Jaringan Komputer

Mg ke-	Kemampuan Akhir Tiap Tahapan Belajar (Sub-CPMK)	Penilaian		Bentuk Pembelajaran; Metode Pembelajaran; Penugasan Mahasiswa; Estimasi Waktu		Materi Pembelajaran	Bobot Penilaian (%)
		Indikator	Bentuk Penilaian	Luring	Daring		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Sub-CPMK1	Mampu menjelaskan pengertian Cyber Security	Kuis, diskusi	a. Kuliah b. Diskusi kasus siber nasional c. Ringkasan teori	Forum diskusi: Definisi & urgensi cyber security	Stallings (2020), Ch. 1	5%
2	Sub-CPMK1	Menjelaskan prinsip dasar keamanan	Kuis, Tugas	a. Kuliah b. Case method: Cyber kill chain c. Tugas individu	Video pembelajaran + kui	Stallings (2020), Ch. 2	5%
3	Sub-CPMK2	Mengidentifikasi jenis ancaman	Tugas tertulis	a. Kuliah b. Pemecahan kasus c. Tugas analisis ancaman	Worksheet identifikasi ancaman	Choraś (2020), Ch. 3	5%
4	Sub-CPMK2	Menjelaskan kerentanan sistem	Quiz, Tugas Kelompok	a. Kuliah b. Diskusi kelompok c. Tugas pemetaan risiko	Penugasan Google Form	Stallings (2020), Ch. 4	5%

5	Sub-CPMK3	Menganalisis serangan siber	Studi kasus	a. Kuliah b. Case method c. Presentasi studi kasus	Google Docs Collaborative Analysis	Anderson (2020), Ch. 5	15%
6	Sub-CPMK3	Menganalisis dampak serangan	Ujian formatif	a. Kuliah b. Simulasi serangan c. Tugas analisis dampak	Quiz di LMS	Goodrich (2014), Ch. 3	5%
7	Sub-CPMK4	Menerapkan kriptografi dasar	Praktik sederhana, evaluasi pemahaman	a. Kuliah b. Proyek mini c. Tugas praktik kriptografi	Simulasi enkripsi Caesar Cipher	Stallings (2020), Ch. 9	10%
8	Sub-CPMK5	Mendesain pengamanan jaringan	Tugas proyek awal	a. Kuliah b. Proyek jaringan sederhana c. Desain Topologi	Video tutorial packet tracer	Choraś (2020), Ch. 6	5%
9	Sub-CPMK5	Menerapkan firewall & IDS sederhana	Praktik & evaluasi jaringan	a. Kuliah b. Praktikum c. Tugas implementasi	Penugasan simulasi	Anderson (2020), Ch. 7	5%
10	Sub-CPMK6	Menyusun dokumen kebijakan keamanan	Draft dokumen	a. Kuliah b. Project-based c. Tugas kebijakan	Kolaborasi Google Docs	Whitman & Mattord (2021), Ch. 8	10%
11	Sub-CPMK6	Review dan diskusi kebijakan keamanan	Presentasi dan peer-review	a. Kuliah b. Presentasi c. Tugas review dan revisi	Forum review dokumen	Whitman & Mattord (2021), Ch. 9	5%
12	Sub-CPMK7	Integrasi keamanan dalam proyek sistem	Proposal proyek akhir	a. Kuliah b. Bimbingan proyek c. Proposal proyek	Draft proposal	Referensi umum pengembangan sistem + keamanan	5%
13	Sub-CPMK7	Pengembangan proyek keamanan	Implementasi sistem	a. Proyek berbasis keamanan b. Studi lapangan jika memungkinkan	Presentasi progres proyek	Dokumentasi proyek keamanan	5%
14	Sub-CPMK7	Penyelesaian proyek dan evaluasi	Presentasi final	a. Presentasi proyek akhir b. Diskusi dan evaluasi kelompok	Upload laporan akhir	Seluruh hasil proyek mahasiswa	10%
15	Refleksi dan Evaluasi Pembelajaran Keseluruhan	Merefleksikan capaian pembelajaran dan pengalaman proyek	Refleksi individu, survei pembelajaran	a. Diskusi kelas b. Pengisian survey refleksi manual	Forum refleksi + survei Google Form	Rekapitulasi seluruh materi & pengalaman proyek	5%
16							

SISTEM PENILAIAN DAN SISTEM EVALUASI

A. Sistem Penilaian

1. Sistem penilaian menggunakan penilaian acuan pokok pada RPS.
2. Komponen, bobot, dan rentang penilaian sebagai berikut:
 - Komponen: nilai kompetensi (CPMK) sebesar 90% dan nilai kehadiran sebesar 10%.

- Nilai akhir mata kuliah = jumlah nilai CPMK + nilai kehadiran.
- Bobot masing-masing CPMK dan kehadiran dapat dilihat pada tabel berikut:

No.	Kompetensi dan Kehadiran	Bobot Penilaian						Target Pengukuran	
		Tugas (10%)	Quiz (10%)	UTS (15%)	UAS (15%)	Case Based (50%)	Kehadiran	Maksimal	Konversi
1.	CPMK-1	2%	2%	3%	3%	10%		20%	A
2.	CPMK-2	2%	2%	3%	3%	10%		20%	A
3.	CPMK-3	2%	2%	3%	3%	10%		20%	A
4.	CPMK-4	2%	2%	3%	3%	10%		20%	A
5.	CPMK-5	2%	2%	3%	3%	10%		20%	A
6.	Kehadiran						0%		A
TOTAL		10%	10%	15%	15%	50%	0%	100%	

Rentang penilaian huruf mengikuti tabel berikut.

No.	Rentang Nilai Angka Skala 100	Nilai Angka Skala 4	Nilai Huruf
1.	80,00 – 100,00	4,00	A
2.	68,00 – 79,99	3,00	B
3.	56,00 – 67,99	2,00	C
4.	45,00 – 55,99	1,00	D
5.	00,00 – 44,99	0,00	E

B. Sistem Evaluasi

1. Mahasiswa dinyatakan lulus dalam mata kuliah ini bila nilai minimal D.
2. Nilai kehadiran mahasiswa dalam perkuliahan harus lebih dari 75%, bila kurang dari nilai tersebut maka nilai otomatis E