	Universitas Negeri Surabaya Fakultas Teknik Program Studi S1 Sistem Informasi	Kode Dokumen

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (sks)			SEMESTER	Tgl Penyusunan
Keamanan SI Berbasis Siber	5720103174		T=3	P=0	ECTS=4.77	4	11 April 2025

OTORISASI	Pengembang RPS	Koordinator RMK	Koordinator Program Studi
	.....	.....	I Kadek Dwi Nuryana, S.T., M.Kom.

Model Pembelajaran: Case Study

Capaian Pembelajaran (CP)

CPL-PRODI yang dibebankan pada MK

CPL-8	Mampu membuat perencanaan infrastruktur TI, arsitektur jaringan, layanan fisik dan cloud, menganalisa konsep identifikasi, otentikasi, otorisasi akses dalam konteks melindungi orang dan perangkat
CPL-13	Mampu memahami dan menjelaskan konsep dan pentingnya keamanan sistem informasi dalam mengelola data dan informasi serta mengidentifikasi hal - hal tentang kebocoran data

Capaian Pembelajaran Mata Kuliah (CPMK)

CPMK - 1	Mampu memahami konsep keamanan informasi berbasis siber dan mengevaluasi cyber security dalam berbagai area, termasuk yang berkaitan dengan ragam ancaman dan kerentanan, aset dan risiko, teknologi keamanan data, teknologi keamanan jaringan atau tata kelola cyber security
CPMK - 2	Memahami teknik-teknik pengamanan data dan jaringan serta menguasai teori dan konsep yang mendasari ilmu computer khususnya cyber security
CPMK - 3	Mampu memahami dan mengembangkan startegi manajemen risiko keamanan informasi serta mampu memahami dan menentukan pendekatan sistem syber security yang sesuai dengan problem yang dihadapi, serta dapat memilih representasi pengetahuan dan mekanisme penalarannya
CPMK - 4	Mengimplementasikan keamanan sistem informasi dalam lingkungan bisnis

Matrik CPL - CPMK

CPMK	CPL-8	CPL-13
CPMK-1		✔
CPMK-2		✔
CPMK-3		✔
CPMK-4	✔	

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									✔	✔	✔			✔	✔	✔

Deskripsi Singkat MK: Mata kuliah ini membahas prinsip-prinsip dan praktik keamanan dalam sistem informasi berbasis siber. Mahasiswa akan mempelajari teknik-teknik pengamanan data dan jaringan, manajemen risiko keamanan informasi, serta strategi untuk melindungi sistem informasi dari ancaman siber. Fokus juga diberikan pada kebijakan, teknologi keamanan, dan penerapan solusi keamanan dalam lingkungan bisnis.

Pustaka

Utama :

1. Computer Security: Principles and Practice oleh William Stallings dan Lawrie Brown.
2. Cybersecurity Essentials oleh Charles J. Brooks, et al
3. Risk Management Framework: A Lab-Based Approach to Securing Information Systems oleh James Broad.
4. Data and Computer Security: Principles and Practice oleh John W. Rittinghouse dan James F. Ransome.
5. Practical Network Security: Securing Your Network Against Cyber Attacks oleh Michael Gregg.
6. Information Security Management Handbook oleh Harold F. Tipton dan Micki Krause.
7. Information Security Risk Management: A Comprehensive Guide to Protecting Your Assets oleh Steve B. McLaughlin.
8. Cyber Security and IT Infrastructure Protection oleh Thomas J. Gannon.
9. Introduction to the Theory of Computation oleh Michael Sipser.
10. Knowledge Representation and Reasoning oleh Ronald Brachman dan Hector Levesque.
11. The Art of Deception: Controlling the Human Element of Security oleh Kevin D. Mitnick dan William L. Simon.
12. The Cybersecurity Handbook: A Step-by-Step Guide for Executives oleh Omar Santos dan Joseph Steinberg.
13. Implementing Information Security Based on ISO 27001/ISO 27002 oleh Alan Calder.
14. Security Risk Management: Building an Information Security Risk Management Program oleh Evan Wheeler.

Pendukung :

Dosen Pengampu	

Mg Ke-	Kemampuan akhir tiap tahapan belajar (Sub-CPMK)	Penilaian		Bantuk Pembelajaran, Metode Pembelajaran, Penugasan Mahasiswa, [Estimasi Waktu]		Materi Pembelajaran [Pustaka]	Bobot Penilaian (%)
		Indikator	Kriteria & Bentuk	Luring (*offline*)	Daring (*online*)		
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Mampu memahami dan menjelaskan konsep dasar keamanan informasi berbasis siber dan perannya dalam era digital	1.Dapat memahami dan menjelaskan definisi keamanan informasi berbasis siber 2.Dapat memahami dan mengidentifikasi peran penting keamanan siber dalam melindungi data di era digital dan dapat memberikan contoh implementasi keamanan siber dalam berbagai konteks digital	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Aktifitas Partisipasif	Diskusi kelas tentang konsep dasar keamanan informasi berbasis siber melalui studi kasus, diikuti dengan penugasan individu untuk membuat esai. 3 X 50	Memahami konsep dasar keamanan siber dengan studi kasus, diikuti dengan penugasan individu untuk menulis esai dan mengunggahnya secara online. 3 X 50	**Materi:** Konsep dasar keamanan informasi berbasis siber, pentingnya keamanan siber dalam era digital. **Pustaka:** *Computer Security: Principles and Practice oleh William Stallings dan Lawrie Brown.*	2%
2	Mampu memahami dan mengidentifikasi berbagai jenis ancaman siber dan kerentanan dalam sistem informasi	1.Dapat memahami dan mengidentifikasi serta menjelaskan berbagai ancaman siber, dapat mengklasifikasikan jenis-jenis kerentanan dalam sistem informasi 2.Ketepatan mahasiswa dalam memberikan contoh bagaimana kerentanan dieksploitasi oleh ancaman siber	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Aktifitas Partisipasif	Analisis kelompok terhadap jenis ancaman siber dalam diskusi kelas, dengan tugas presentasi kelompok. 3 X 50	Diskusi kelompok tentang jenis ancaman siber menggunakan platform kolaborasi online, dengan penugasan untuk membuat dan mengunggah video presentasi. 3 X 50	**Materi:** Jenis-jenis ancaman siber dan kerentanan dalam sistem informasi. **Pustaka:** *Cybersecurity Essentials oleh Charles J. Brooks, et al*	3%
3	Mampu memahami dan mnegevaluasi asset dan risiko dalam koteks keamanan siber	1.Mampu memahami dan mengidentifikasi asset informasi penting dalam organisasi dan dapat menganalisisi risiko yang terkait dengan set informasi 2.Dapat mengevaluasi dampak risiko dan enentukan prioritas	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk	Evaluasi risiko dan aset keamanan siber melalui diskusi kasus di kelas, disertai tugas laporan individu. 3 X 50	Analisis risiko siber melalui diskusi kasus di forum online, diikuti penugasan individu untuk membuat laporan dan mengunggahnya. 3 X 50	**Materi:** Evaluasi aset dan risiko dalam keamanan siber. **Pustaka:** *Risk Management Framework: A Lab-Based Approach to Securing Information Systems oleh James Broad.*	3%
4	Mampu memahami dan menerapkan teknologi keamanan data dalam melindungi informasi	1.Dapat memahami dan menjelaskan konsep dasar enkripsi dalam keamanan data 2.Dapat menerapkan teknik enkripsi dan deskripsi pada data sensitive serta mendemostrasikan cara kerja teknologi tokenisasi dalam melindungi data	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk	Praktikum di laboratorium tentang teknologi keamanan data, dengan penugasan proyek kelompok. 3 X 50	Praktikum menggunakan simulasi software keamanan data, dengan penugasan proyek kelompok yang diunggah di platform e-learning. 3 X 50	**Materi:** Teknologi keamanan data, enkripsi, dan perlindungan data. **Pustaka:** *Data and Computer Security: Principles and Practice oleh John W. Rittinghouse dan James F. Ransome.*	3%
5	Mampu memahami dan menerapkan teknologi keamanan jaringan	1.Dapat memahami dan menjelaskan prinsip kerja firewall, IDS/IPS dan VPN 2.Dapat mengkonfigurasi firewall dasar untuk melindungi jaringan dari ancaman	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk	Simulasi keamanan jaringan di lab, diikuti dengan tugas konfigurasi jaringan dalam kelompok. 3 X 50	Simulasi keamanan jaringan melalui aplikasi jaringan virtual, dengan penugasan konfigurasi dan pengujian yang diunggah online.	**Materi:** Teknologi keamanan jaringan, firewall, IDS/IPS. **Pustaka:** *Practical Network Security: Securing Your Network Against Cyber Attacks oleh Michael Gregg.*	3%
6	Mampu memahami dan mnegevaluasi tata kelola keamanan infromasi dalam organisasi	Dapat mejelaskan prinsip-prinsip tata kelola keamanan informasi dan dapat mengidentifikasi elemen penting dari kebijakan keamanan informasi	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk	Diskusi kelas mengenai tata kelola keamanan informasi dalam organisasi, disertai laporan evaluasi kelompok. 3 X 50	Diskusi kelompok secara daring tentang tata kelola keamanan informasi, diikuti dengan laporan evaluasi yang dikumpulkan secara online. 3 X 50	**Materi:** Tata kelola keamanan informasi dalam organisasi, kebijakan dan prosedur. **Pustaka:** *Information Security Management Handbook oleh Harold F. Tipton dan Micki Krause.*	3%

7	Mampu memahami dan mengembangkan strategi manajemen risiko keamanan infromasi	Dapat menyusun strategi manajemen risiko, dan menerapkan teknik penilaian risiko	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk	Pengembangan strategi manajemen risiko dalam diskusi kelas, dengan tugas proposal kelompok. 3 X 50	Memahami strategi manajemen risiko, diikuti dengan penugasan membuat proposal dan mengunggahnya. 3 X 50	**Materi:** Strategi manajemen risiko keamanan informasi. **Pustaka:** *Information Security Risk Management: A Comprehensive Guide to Protecting Your Assets oleh Steve B. McLaughlin.*	3%
8			**Bentuk Penilaian** : Tes	UTS 3 X 50	UTS 3 X 50	**Materi:** UTS **Pustaka:**	0%
9	Mampu memahami dan memilih serta menerapkan pendekatan keamanan siber	1.Dapat memahami dan membandingkan berbagai pendekatan keamanan siber dan dapat memilih pedekatan yang paling sesuai dengan masalah keamanan teretntu 2.Ketepatan mahasiswa dalam menerapkan pendekatan tersebut dalam studi kasus nyata	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Aktifitas Partisipasif	Studi kasus di kelas tentang pendekatan keamanan siber, diikuti dengan penugasan proyek kelompok. 3 X 50	Analisis studi kasus secara daring tentang pendekatan keamanan siber, disertai dengan penugasan proyek yang dikumpulkan secara online. 3 X 50	**Materi:** Pendekatan keamanan siber yang berbeda, strategi perlindungan. **Pustaka:** *Cyber Security and IT Infrastructure Protection oleh Thomas J. Gannon.*	4%
10	Mampu memahami dan menjelaskan konse dan teori dasar dalam ilmu computer terkait keamanan siber	1.Dapat menjelaskan teoi-teori dasar seperto model ancaman, kriptografi, dan control akses 2.Dapat memahami dan menjelaskan penerapan teori-teori dalam scenario keamanan siber 3.Ketepatan mahasiswa dalam memberikan contoh implementasi teoridalam keamanan sistem informasi	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Aktifitas Partisipasif	Memahami konsep dasar ilmu komputer dalam keamanan siber, dengan tugas esai individu. 3 X 50	Memahami konsep dasar ilmu komputer dalam keamanan siber, diikuti dengan penugasan esai yang diunggah ke platform. 3 X 50	**Materi:** Konsep dasar dalam ilmu komputer terkait keamanan siber. **Pustaka:** *Introduction to the Theory of Computation oleh Michael Sipser.*	4%
11	Mampu memahami dan menerapkan representasi pengetahuan dan mekanisme dalam keamanan siber	Dapat memahami dan menjelaskan konsep representasi pengetahuan seperti logika fuzzy dan menerapkan mekanisme penalaran untuk mendeteksi ancaman siber	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Aktifitas Partisipasif, Penilaian Hasil Project / Penilaian Produk	Diskusi dan praktik di kelas mengenai representasi pengetahuan dan mekanisme penalaran, dengan tugas individu untuk membuat model. 3 X 50	Memahami representasi pengetahuan dalam keamanan siber, dengan penugasan membuat model dan mengunggahnya. 3 X 50	**Materi:** Representasi pengetahuan dan mekanisme penalaran dalam keamanan siber. **Pustaka:** *Knowledge Representation and Reasoning oleh Ronald Brachman dan Hector Levesque.*	4%
12	Mampu memahami dan mengembangkan startegi dalam menghadapi ancaman siber	1.Dapat mengidentifikasi berbagai ancaman siber yang berkembang dan dapat mengembangkanstrategi untuk mitigasi dan respons terhadap ancaman siber 2.Ketepatan mahassiswa dalam menerapkan startegi tersebut dalam lingkungan nyata atau simulasi	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk	Diskusi kelas tentang strategi menghadapi ancaman siber, diikuti tugas kelompok untuk mengembangkan strategi. 3 X 50	Diskusi kelompok secara daring mengenai strategi ancaman siber, disertai dengan tugas pengembangan strategi yang diunggah. 3 X 50	**Materi:** Strategi untuk menghadapi ancaman siber, mitigasi dan penanggulangan. **Pustaka:** *The Art of Deception: Controlling the Human Element of Security oleh Kevin D. Mitnick dan William L. Simon.*	4%
13	Mampu memahami pedekatan dan teknik terbaru dalam cyber security		**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Aktifitas Partisipasif	Memahami teknik terbaru dalam cyber security, dengan tugas membuat makalah individu. 3 X 50	Memahami teknik terbaru dalam cyber security, diikuti dengan penugasan makalah yang diunggah ke platform e-learning. 3 X 50	**Materi:** Teknik terbaru dalam cyber security, tren dan perkembangan. **Pustaka:** *The Cybersecurity Handbook: A Step-by-Step Guide for Executives oleh Omar Santos dan Joseph Steinberg.*	4%

14	Mampu memahami dan merancang serta mengimplementasikan sistem keamanan siber yang efektif dalam lingkugan bisnis	1.Dapat memahami dan merancang sistem keamanan yang disesuaikan dengan kebutuhan bisnis dan dapat menerapkan sistem keamanan yang telah dirancang dalam lingkungan bisnis 2.Dapat mengevaluasi efektivitas sistem keamanan yang telah diimplementasikan	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Praktik / Unjuk Kerja	Proyek kelompok di kelas untuk merancang dan mengimplementasikan sistem keamanan siber, dengan presentasi hasil proyek. 3 X 50	Proyek kelompok daring untuk merancang dan mengimplementasikan sistem keamanan siber, dengan presentasi hasil yang diunggah dalam format video. 3 X 50	**Materi:** Perancangan dan implementasi sistem keamanan siber dalam bisnis. **Pustaka:** *Implementing Information Security Based on ISO 27001/ISO 27002 oleh Alan Calder.*	5%
15	Mampu mengevaluasi dan mengoptimalkan sistem keamanan yang telah dirancang dan diimplementasikan	1.Dapat melakukan penilaian ulang etrhadap sistem keamanan yang telah ada dan dapat mengidentifikasi area untuk perbaikan dan optimasi 2.Ketepatan mahassiwa dalam mengimplementasikan perubahanyang dipelukan untuk meningkatkan keamana sistem.	**Kriteria:** 1.Tes Kognitif 2.Partisipasi = 20% 3.Tugas = 30% 4.UTS = 20% 5.UAS = 30% **Bentuk Penilaian** : Penilaian Hasil Project / Penilaian Produk, Praktik / Unjuk Kerja	Evaluasi dan optimasi sistem keamanan yang telah dirancang melalui diskusi kelas, dengan laporan kelompok. 3 X 50	Evaluasi dan optimasi sistem keamanan secara daring melalui diskusi virtual, disertai laporan kelompok yang diunggah secara online. 3 X 50	**Materi:** Evaluasi dan optimasi sistem keamanan siber yang telah diimplementasikan. **Pustaka:** *Security Risk Management: Building an Information Security Risk Management Program oleh Evan Wheeler.*	5%
16			**Bentuk Penilaian** : Tes	UAS 3 X 50	UAS 3 X 50	**Materi:** UAS **Pustaka:**	30%

Rekap Persentase Evaluasi : Case Study

No	Evaluasi	Persentase
1.	Aktifitas Partisipasif	20.5%
2.	Penilaian Hasil Project / Penilaian Produk	24.5%
3.	Praktik / Unjuk Kerja	5%
4.	Tes	30%
		80%

Catatan

1. **Capaian Pembelajaran Lulusan Prodi (CPL - Prodi)** adalah kemampuan yang dimiliki oleh setiap lulusan prodi yang merupakan internalisasi dari sikap, penguasaan pengetahuan dan ketrampilan sesuai dengan jenjang prodinya yang diperoleh melalui proses pembelajaran.
2. **CPL yang dibebankan pada mata kuliah** adalah beberapa capaian pembelajaran lulusan program studi (CPL-Prodi) yang digunakan untuk pembentukan/pengembangan sebuah mata kuliah yang terdiri dari aspek sikap, ketrampulan umum, ketrampilan khusus dan pengetahuan.
3. **CP Mata kuliah (CPMK)** adalah kemampuan yang dijabarkan secara spesifik dari CPL yang dibebankan pada mata kuliah, dan bersifat spesifik terhadap bahan kajian atau materi pembelajaran mata kuliah tersebut.
4. **Sub-CPMK Mata kuliah (Sub-CPMK)** adalah kemampuan yang dijabarkan secara spesifik dari CPMK yang dapat diukur atau diamati dan merupakan kemampuan akhir yang direncanakan pada tiap tahap pembelajaran, dan bersifat spesifik terhadap materi pembelajaran mata kuliah tersebut.
5. **Indikator penilaian** kemampuan dalam proses maupun hasil belajar mahasiswa adalah pernyataan spesifik dan terukur yang mengidentifikasi kemampuan atau kinerja hasil belajar mahasiswa yang disertai bukti-bukti.
6. **Kreteria Penilaian** adalah patokan yang digunakan sebagai ukuran atau tolok ukur ketercapaian pembelajaran dalam penilaian berdasarkan indikator-indikator yang telah ditetapkan. Kreteria penilaian merupakan pedoman bagi penilai agar penilaian konsisten dan tidak bias. Kreteria dapat berupa kuantitatif ataupun kualitatif.
7. **Bentuk penilaian:** tes dan non-tes.
8. **Bentuk pembelajaran:** Kuliah, Responsi, Tutorial, Seminar atau yang setara, Praktikum, Praktik Studio, Praktik Bengkel, Praktik Lapangan, Penelitian, Pengabdian Kepada Masyarakat dan/atau bentuk pembelajaran lain yang setara.
9. **Metode Pembelajaran:** Small Group Discussion, Role-Play & Simulation, Discovery Learning, Self-Directed Learning, Cooperative Learning, Collaborative Learning, Contextual Learning, Project Based Learning, dan metode lainnya yg setara.
10. **Materi Pembelajaran** adalah rincian atau uraian dari bahan kajian yg dapat disajikan dalam bentuk beberapa pokok dan sub-pokok bahasan.
11. **Bobot penilaian** adalah prosentasi penilaian terhadap setiap pencapaian sub-CPMK yang besarnya proposional dengan tingkat kesulitan pencapaian sub-CPMK tsb., dan totalnya 100%.
12. TM=Tatap Muka, PT=Penugasan terstruktur, BM=Belajar mandiri.

RPS ini telah divalidasi pada tanggal 20 Desember 2024

Koordinator Program Studi S1 Sistem Informasi

I Kadek Dwi Nuryana, S.T., M.Kom.
NIDN 0014048107

UPM Program Studi S1 Sistem Informasi

Anggraeni Widya Purwita, M.Kom.
NIDN 0008029505

VALID