	Universitas Negeri Surabaya Fakultas Vokasi Program Studi D4 Manajemen Informatika	Kode Dokumen

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (sks)			SEMESTER	Tgl Penyusunan
Prak. Keamanan Perangkat Lunak	5730102190		T=0	P=2	ECTS=3.18	5	24 Januari 2026

OTORISASI	Pengembang RPS	Koordinator RMK	Koordinator Program Studi
	.....	.....	DODIK ARWIN DERMAWAN

Model Pembelajaran	**Case Study**
Capaian Pembelajaran (CP)	**CPL-PRODI yang dibebankan pada MK**
	Capaian Pembelajaran Mata Kuliah (CPMK)
	Matrik CPL - CPMK

	CPMK

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

Deskripsi Singkat MK	Dalam matakuliah ini dibahas tentang hal-hal yang harus diperhatikan dandilakukan dalam menerapkan keamanan perangkat lunak. Sejumlah aspek lain yang relevan juga turut dibahas seperti manajemen resiko perangkat lunak dan evaluasi kontrol perangkat lunak.
Pustaka	**Utama :**

1. Camplbell, Tony. 2016. Practical Information Security Management: A Complete Guide to Planning and Implementation,Burns Beach,Australia
2. Kemenkominfo, 2015, INDEKS KAMI. JAKARTA

Pendukung :

Dosen Pengampu	Asmunin, S.Kom., M.Kom. I Gde Agung Sri Sidhimantra, S.Kom., M.Kom.

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	Evolusi Profesi	1.sejarah profesi keamanan perangkat lunak 2.Risiko dan Konsekuensi	**Kriteria:** Rubrik Holistik	Pendekatan: Saintifik Model: Kooperatif Metode: Diskusi, Presentasi 2 X 50			0%

2	Ancaman dan Kerentanan Keamanan perangkat lunak	1.Ancaman 2.Kerentanan 3.Kecanggihan dan kemampuan penjahat dunia maya sekarang lebih besar daripada sebelumnya, dengan pelaku ancaman teknis yang unggul yang meneliti dan mengembangkan kerangka kerja malware berbahaya yang memungkinkan mereka atau Pelanggan mereka untuk masuk ke sistem korban mereka, menjaga akses, menutupi jejak mereka, menghindari tindakan balasan dan menyedot gigabyte informasi rahasia untuk dijual di pasar gelap. Bab ini membahas berbagai ancaman dan kerentanan yang mempengaruhi kita setiap hari, termasuk yang buatan manusia dan ancaman alami yang sering diabaikan saat mempertimbangkan keamanan informasi.	**Kriteria:** Rubrik Holistik	Pendekatan: Saintifik Model: Kooperatif Metode: Diskusi, Presentasi 2 X 50			0%

3	Manajer Keamanan	1. Role dari manajer kemanan perangkat lunak 2. pengembangan karier 3. cara menjadi manajer keamanan perangkat lunak 4. Menyelami peran manajer keamanan perangkat lunak dan melihat apa yang harus mereka lakukan Dari hari ke hari. Kami juga berfokus pada bagaimana manajer keamanan perangkat lunak dapat mengelola keterampilan dan kompetensi tim mereka dengan menggunakan kerangka kerja keterampilan yang diakui dan bagaimana profesionalisme dalam sektor keamanan dapat digunakan untuk mengangkat semua peran kami sebagai petugas keamanan dari lingkup TI tradisional menjadi sebuah profesi. Semua miliknya sendiri. Kami juga akan melihat beberapa mitos umum dan kesalahpahaman yang terkait dengan kursus pelatihan profesional dan kursus akademis dan kaitannya dengan rencana pengembangan karir Anda, menutup bab ini dengan melihat sekilas apa itu sistem manajemen keamanan perangkat lunak.	**Kriteria:** Rubrik Holistik	Pendekatan: Saintifik Model: KooperatifMetode: Diskusi, Presentasi 2 X 50			0%

4	Keamanan Perangkat Lunak sebagai Fungsi Bisnis	1.Keamanan dalam Struktur Organisasi 2.Bekerja dengan Kelompok Spesialis 3.Bekerja dengan Standar dan Peraturan 4.Bekerja dengan Manajemen Risiko 5.Bekerja dengan Arsitektur Enterprise 6.Bekerja dengan Manajemen Fasilitas 7.melihat bagaimana manajer keamanan perangkat lunak dapat menanamkan keamanan sebagai fungsi dalam bisnis, memastikan bahwa kita menyelaraskan semua orang, proses, dan teknologi ke hasil keamanan yang mendukung bisnis dan kebutuhan strategisnya. Kita akan melihat struktur organisasi tradisional yang kita lihat setiap hari dalam bisnis, melihat bagaimana memberi lapisan keamanan ke dalam struktur ini untuk memastikan bahwa kita mencakup semua aspek risiko, tidak hanya yang terkait dengan cyber. Bab ini membahas manajemen risiko, manajemen kontinuitas bisnis dan arsitektur enterprise yang lebih dalam, yang menjelaskan peran keamanan dalam masing-masing fungsi bisnis ini. Bab ini ditutup dengan penjelasan singkat tentang bagaimana keamanan dapat diintegrasikan dengan manajemen fasilitas	**Kriteria:** Rubrik Holistik	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50			0%

5	Implementasi Keamanan perangkat lunak	1. Integrasi dengan Manajemen Risiko 2. Bahasa Resiko 3. Gunakan Kerangka yang Ada 4. Pengembangan Aman 5. Kesadaran Arsitektur Keamanan 6. Persyaratan Keamanan 7. Antarmuka Organisasi 8. Implementasi keamanan perangkat lunak masuk ke rincian lebih lanjut tentang bagaimana manajer keamanan perangkat lunak dapat mengintegrasikan fungsi tim keamanan dengan fungsi yang disediakan oleh organisasi lainnya, seperti manajemen risiko, arsitektur dan pengembangan perangkat lunak. Yang terpenting, bab ini terlihatPada konsep persyaratan keamanan yang bertentangan dengan kontrol keamanan, menunjukkan kepada Anda bagaimana untuk mendapatkan persyaratan keamanan di tahap inisiasi proyek untuk memastikan bahwa ancaman, kerentanan, dan risiko ditangani oleh desain dan bukan sebagai renungan.	**Kriteria:** Rubrik Holistik	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50			0%
6							0%

7	Kerangka Standar Pedoman dan Perundang-undangan	1. Mengapa Kita Membutuhkan Standar? 2. Perundang-undangan 3. Standar Standar ISO / IEC 27000 4. Keberlangsungan bisnis 5. Standar Manajemen Risiko 6. COBIT 7. Sebagai dasar dari segala hal yang kita lakukan dalam keamanan, terutama saat beroperasi dalam peran manajer keamanan informasi, kita perlu membenarkan apa yang kita memaksakan bisnis dari sudut pandang pengurangan risiko. Di dunia di mana ancaman dan kerentanan mempengaruhi apa yang kita lakukan setiap hari, sekarang ada banyak standar, kerangka kerja, pedoman dan undang-undang nasional yang mendorong apa yang harus kita lakukan untuk memenuhi persyaratan industri atau hukum tertentu. Bab 6 membahas berbagai standar dan pedoman internasional yang mempengaruhi organisasi kita, menilai nilai mereka kepada Anda sebagai manajer keamanan informasi dan juga nilai mereka untuk industri secara umum.	**Kriteria:** Rubrik Holistik	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 6 X 50			0%
8	UTS / USS			2 X 50			0%
9							0%
10							0%

11	Perlindungan Informasi	1.Klasifikasi Informasi 2.Tingkat Dampak Bisnis 3.Melaksanakan Klasifikasi Informasi 4.Implementasi Strategis 5.Identifikasi, Otentikasi, dan Otorisasi 6.Model Kontrol Akses 7.Sistem Wewenang 8.Delegasi Hak Istimewa 9.Informasi adalah sumber kehidupan bisnis modern, tidak peduli apakah mereka melakukan perdagangan asuransi perjalanan, rahasia pemerintah, bangunan, dan konstruksi atau informasi pendidikan lanjutan berada di jantung usaha membuat bisnis ini berjalan. Bab 7 melihat bagaimana kita dapat membangun sistem untuk membantu melindungi informasi penting yang sangat penting dalam organisasi kita, dengan mempertimbangkan kepekaan data dan sistem kontrol akses yang dapat kita gunakan untuk memastikan bahwa hanya mereka yang perlu mengakses mendapatkannya.	**Kriteria:** Rubrik Holistik	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50			0%
12	Perlindungan Orang	1.Kerentanan Manusia 2.Teknik Sosial 3.Membangun Budaya Keamanan 4.Staf lalai 5.Aturan Berselancar dan Menguping 6.Perilaku Kode 7.Employment Contracts 8.Siklus Hidup Keamanan Personalia 9.Pengerahan 10.Pilihan 11.Kinerja dan Suksesi 12.Transisi	**Kriteria:** Rubrik Holistik	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50			0%

13	Protection of Premises	1.Apa itu Keamanan Fisik? 2.Keamanan Fisik di ISO / IEC 27001: 2013 3.Mulailah dengan Risk Assessment 4.Ancaman dan Kerentanan 5.Lengkapi Risk Assessment 6.Perimeter Desain 7.Hambatan, Dinding, dan Pagar 8.Mailrooms dan Loading Bays 9.Penjaga keamanan 10.CCTV 11.Penerangan 12.Kantor, lokasi lapangan, dan pusat data semuanya bisa menjadi titik lemah dalam operasi dimana serangan dapat terjadi. Di pertemuan ini kita melihat tindakan pengamanan fisik yang dapat kita ambil untuk membela dan mempertahankan fasilitas kita, termasuk pertimbangan utama yang harus dimiliki manajer keamanan informasi saat bekerja bersama para ahli di tim manajemen fasilitas, eksekutif bisnis dan penegakan hukum untuk membantu melindungi fisik kita. Lingkungan.	**Kriteria:** Rubrik Holistik	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 4 X 50			0%
14							0%

15	Protection of Systems	1.Memperkenalkan Malware 2.Apa itu Malware? 3.Klasifikasi Perangkat Lunak Perusak 4.Serangan Konten Aktif 5.Vektor ancaman 6.Penanggulangan Teknis 7.Keamanan jaringan 8.Apakah Firewall itu? 9.Zona Demiliterisasi (DMZ) 10.Enkripsi Jaringan 11.Jaringan nirkabel 12.kontrol teknis yang perlu diketahui oleh manajer keamanan informasi di dalam arsitektur enterprise, memastikan dasar pengetahuan keamanan yang masuk akal dapat ditambahkan ke gudang keamanan. Ini akan membantu manajer keamanan informasi saat mereka melakukan percakapan dengan tim teknis, seperti insinyur jaringan, pakar sistem operasi Windows dan administrator basis data, memastikan manajer keamanan informasi dapat berbicara bahasa mereka sambil menerjemahkan risiko teknis ke dalam kontrol keamanan yang berarti.	**Kriteria:** Rubrik Holistik	Pendekatan:Saintifik Model: KooperatifMetode:Diskusi, Presentasi 2 X 50			0%
16	UAS			2 X 50			0%

Rekap Persentase Evaluasi : Case Study

No	Evaluasi	Persentase
		0%

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.