



**Universitas Negeri Surabaya
Fakultas Ekonomika dan Bisnis
Program Studi S1 Bisnis Digital**

Kode
Dokumen

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	KODE	Rumpun MK	BOBOT (sks)	SEMESTER	Tgl Penyusunan
Data Security Management	6120903026	Mata Kuliah Pilihan Program Studi	T=0 P=0 ECTS=0	4	8 April 2025
OTORISASI	Pengembang RPS		Koordinator RMK	Koordinator Program Studi	
	Renny Sari Dewi S.Kom., M.Kom		Ika Diyah Candra Arifah S.E., M.Com, CMA	Hujjatullah Fazlurrahman, S.E., MBA.	

Model Pembelajaran	Case Study
---------------------------	------------

Capaian Pembelajaran (CP)	CPL-PRODI yang dibebankan pada MK
----------------------------------	--

CPL-3	Mengembangkan pemikiran logis, kritis, sistematis, dan kreatif dalam melakukan pekerjaan yang spesifik di bidang keahliannya serta sesuai dengan standar kompetensi kerja bidang yang bersangkutan
CPL-5	Mampu menguasai teori bidang bisnis digital secara menyeluruh
CPL-6	Mampu beradaptasi terhadap konteks permasalahan bisnis digital yang dihadapi dengan baik
CPL-7	Mampu mengembangkan ide bisnis digital secara kreatif dan inovatif
CPL-8	Mampu mengembangkan keilmuan di bidang bisnis digital dengan tepat
CPL-9	Mampu mengembangkan bisnis digital berdasarkan entrepreneurial leadership secara berkelanjutan
CPL-10	Mampu mengimplementasikan teori bidang bisnis digital dalam mengelola organisasi secara etis dan efektif
CPL-11	Mampu mengaplikasikan teknologi informasi dan komunikasi dalam pengelolaan bisnis dengan tepat

Capaian Pembelajaran Mata Kuliah (CPMK)	
--	--

CPMK - 1	Mahasiswa mampu menjelaskan konsep, kebijakan, dan kaitan keamanan data terhadap penggunaan TI [C2, P2]
CPMK - 2	Mahasiswa mampu memberikan studi kasus dan penjelasan tentang kerangka kerja atau standar internasional yang terkait dengan perlindungan data konsumen [C3, A2]
CPMK - 3	Mahasiswa mampu mempraktikkan teknik penyerangan data melalui media teknologi informasi [C3, P3, A2]
CPMK - 4	Mahasiswa mampu menyikapi dengan bijak pasca penyerangan data secara etis [C3, P2, A3]

Matrik CPL - CPMK	
--------------------------	--

CPMK	CPL-3	CPL-5	CPL-6	CPL-7	CPL-8	CPL-9	CPL-10	CPL-11
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		Seiring berkembangnya ilmu pengetahuan dan teknologi yang makin pesat, maka afeksi dan psikomotorik mahasiswa perlu diberikan wawasan terkait isu global, kerangka kerja, hingga standar nasional/internasional yang bertujuan untuk pengamanan data. Perkuliahan ini dirancang agar mahasiswa mampu mempelajari landasan hukum penggunaan teknologi informasi secara bijak dan etis. Namun dalam perkuliahan ini juga terdapat praktik teknik penyerangan data agar dapat memahami secara komprehensif mengenai pengelolaan keamanan data. Matakuliah ini disampaikan dalam bentuk diskusi, case-based learning, dan bermain peran. Setelah menempuh mata kuliah manajemen keamanan data, mahasiswa diharapkan menyelami peran sebagai peretas data sehingga dapat dijadikan lesson learned agar lebih berhati-hati dalam membagikan data dalam suatu organisasi. (As science and technology develop more rapidly, affective and psychomotor students need to be given insight regarding global issues, frameworks, and national/international standards to secure data. This course is designed so that students can learn the legal basis for the wise and ethical use of information technology. However, in this lecture, there is also the practice of data attack techniques to understand data security management comprehensively. This course is delivered through discussions, case-based learning, and role-playing. After taking the data security management course, students are expected to explore the role of data hackers so that lessons learned can be used to be more careful in sharing data within the organization.)					
Pustaka		Utama : 1. Chopra, A, and Chaudhary, M. Implementing an Information Security Management System, Security Management Based on ISO 27001 Guidelines. 2020 2. ISO/IEC 27001:2013 Information Security Management 3. Framework COBIT 2019 Pendukung : 1. Modul Praktikum Data Security Management					
Dosen Pengampu		Dr. Ratih Amelia, S.E., M.M. Ika Diyah Candra Arifah, S.E., M.Com. Dr Muhammad Fachmi, S.E., M.M. Renny Sari Dewi, S. Kom., M. Kom., MCE., MOS.					
Mg Ke-	Kemampuan akhir tiap tahapan belajar (Sub-CPMK)	Penilaian		Bantuan 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	Mahasiswa mampu memahami konsep tentang manajemen keamanan data/ informasi	1.1.1. Mahasiswa mampu menjelaskan konsep manajemen keamanan data/ informasi 2.1.2. Mahasiswa mengenal keterkaitan antara manajemen keamanan data dengan manajemen risiko 3.1.3. Mahasiswa mampu membedakan keamanan data dan proteksi data	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif	Discovery learning, diskusi 3 X 50	Discovery learning, diskusi 3 X 50	Materi: Konsep Manajemen Risiko Pustaka: Chopra, A, and Chaudhary, M. Implementing an Information Security Management System, Security Management Based on ISO 27001 Guidelines. 2020	2%
2	Mahasiswa mampu menjelaskan kebijakan/ regulasi yang terkait dengan perlindungan data konsumen	1.2.1. Mahasiswa mampu menjelaskan tentang hukum dan etika dalam manajemen keamanan data 2.2.2. Mahasiswa mengenal UU 27 tahun 2022 tentang perlindungan data pribadi (UU PDP)	Kriteria: 5 Bentuk Penilaian : Aktifitas Partisipasif	Discovery learning, diskusi 3 X 50	Discovery learning, diskusi 3 X 50	Materi: Hukum dan etika manajemen sekuritas data Pustaka: Chopra, A, and Chaudhary, M. Implementing an Information Security Management System, Security Management Based on ISO 27001 Guidelines. 2020	2%

3	Mahasiswa mampu menjelaskan penggunaan teknologi informasi secara etis beserta studi kasus yang terkait kebocoran data konsumen	1.3.1. Mahasiswa mampu merangkum kajian literatur terkait manajemen keamanan data konsumen 2.3.2. Mahasiswa mampu menjelaskan adanya kasus kebocoran data 3.3.3. Mahasiswa mampu memberikan solusi atas permasalahan keamanan data	Kriteria: 2 Bentuk Penilaian : Aktifitas Partisipasif	Discovery & Cooperative learning, case-based learning 3 X 50	Discovery & Cooperative learning, case-based learning 3 X 50	Materi: Konsep Manajemen Sekuritas Data/Informasi Pustaka: ISO/IEC 27001:2013 Information Security Management	2%
4	Mahasiswa mampu menjelaskan kerangka kerja atau standar nasional/internasional yang berkaitan dengan perlindungan data konsumen	4.1. Mahasiswa mampu menjelaskan tentang kerangka kerja ISO/IEC 27001	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif	Discovery & Cooperative learning, case-based learning 3 X 50	Discovery & Cooperative learning, case-based learning 3 X 50	Materi: kerangka kerja manajemen sekuritas Pustaka: ISO/IEC 27001:2013 Information Security Management	3%
5	Mahasiswa mampu menjelaskan kerangka kerja atau standar nasional/internasional yang berkaitan dengan perlindungan data konsumen Students can explain national/international frameworks or standards related to consumer data protection	5.1 Mahasiswa mampu menganalisis implementasi ISO/IEC 27001	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif	Discovery & Cooperative learning, case-based learning 3 X 50	Discovery & Cooperative learning, case-based learning	Materi: ISO/IEC 27001 Pustaka: ISO/IEC 27001:2013 Information Security Management	5%
6	Mahasiswa mampu menjelaskan kerangka kerja atau standar nasional/internasional yang berkaitan dengan perlindungan data konsumen	6.1 Mahasiswa mampu menjelaskan kerangka kerja Control Objective for Information Technology (COBIT)	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif	Discovery & Cooperative learning, case-based learning 3 X 50	Discovery & Cooperative learning, case-based learning	Materi: COBIT 2019 Pustaka: Framework COBIT 2019	5%
7	Mahasiswa mampu menjelaskan kerangka kerja atau standar nasional/internasional yang berkaitan dengan perlindungan data konsumen Students can explain national/international frameworks or standards related to consumer data protection	7.1 Mahasiswa mampu menganalisis penerapan kerangka kerja Control Objective for Information Technology (COBIT)	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif, Praktik / Unjuk Kerja	Discovery & Cooperative learning, case-based learning 3 X 50	Discovery & Cooperative learning, case-based learning 3 X 50	Materi: COBIT 2019 Pustaka: Framework COBIT 2019	5%

8	Ujian tengah semester	Mahasiswa mampu menjawab dengan benar dan teliti dari kompilasi materi perkuliahan 1-7	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif, Tes	Tes tulis 3 X 50	Tes tulis 3 x 50	Materi: Konsep Manajemen Sekuritas Pustaka: <i>Chopra, A, and Chaudhary, M. Implementing an Information Security Management System, Security Management Based on ISO 27001 Guidelines. 2020</i> Materi: Pembahasan kasus 1 Pustaka: <i>ISO/IEC 27001:2013 Information Security Management</i> Materi: Pembahasan kasus 2 Pustaka: <i>Framework COBIT 2019</i>	20%
9	Mahasiswa mampu mempraktikkan teknik-teknik penyerangan data konsumen melalui perangkat lunak	1.9.1 Mahasiswa mampu memahami bentuk-bentuk penyerangan terhadap perangkat lunak 2.9.2 Mahasiswa mampu memetakan kelebihan dan kekurangan tools penyerangan perangkat lunak/ media sosial	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif	Praktik komputer, simulasi perangkat lunak 3 X 50	Praktik komputer, simulasi perangkat lunak 3 x 50	Materi: Pengantar dan petunjuk umum praktikum Pustaka: <i>Modul Praktikum Data Security Management</i>	3%
10	Mahasiswa mampu mempraktikkan teknik-teknik penyerangan data konsumen melalui perangkat lunak	10.1 Mahasiswa mampu mempraktikkan tools penyerangan dengan metode SQL Injection	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif	Praktik komputer, simulasi perangkat lunak 3 X 50	Praktik komputer, simulasi perangkat lunak 3 x 50	Materi: SQL injection Pustaka: <i>Modul Praktikum Data Security Management</i>	3%
11	Mahasiswa mampu mempraktikkan teknik-teknik penyerangan data konsumen melalui perangkat lunak	11.1 Mahasiswa mampu mempraktikkan tools penyerangan dengan metode Phishing atau Sniffing	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif	Praktik komputer, simulasi perangkat lunak 3 X 50	Praktik komputer, simulasi perangkat lunak 3 x 50	Materi: Phishing Pustaka: <i>Modul Praktikum Data Security Management</i>	2%
12	Mahasiswa mampu mempraktikkan teknik-teknik penyerangan data konsumen melalui perangkat lunak	12.1 Mahasiswa mampu mempraktikkan tools penyerangan dengan metode Spoofing	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif, Praktik / Unjuk Kerja	Praktik komputer, simulasi perangkat lunak 3 X 50	Praktik komputer, simulasi perangkat lunak 3 x 50	Materi: Spoofing Pustaka: <i>Modul Praktikum Data Security Management</i>	3%

13	Mahasiswa mampu menyebutkan kelemahan perangkat lunak yang menjadi penyebab kebocoran data	13.1 Mahasiswa mampu mengenali bentuk-bentuk hak akses (permission) dalam hal berbagi berkas (file sharing)	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif, Praktik / Unjuk Kerja	3 X 50		Materi: hak akses (permission) dalam hal berbagi berkas (file sharing) Pustaka: Modul Praktikum Data Security Management	5%
14	Mahasiswa mampu menyebutkan kelemahan perangkat lunak yang menjadi penyebab kebocoran data	14.1 Mahasiswa mampu mengkaji kelemahan perangkat lunak yang rawan peretasan/penyerangan	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif, Praktik / Unjuk Kerja	Ceramah, diskusi 3 X 50	Ceramah, diskusi 3 x 50	Materi: File Sharing Pustaka: Modul Praktikum Data Security Management	5%
15	Mahasiswa mampu menyikapi penggunaan teknologi informasi dengan bijak, etis, dan efisien untuk mencegah terjadinya kebocoran data	1.15.1 Mahasiswa mampu membuat kajian ilmiah mengenai teknik pencegahan kebocoran data secara bijak dan etis 2.15.2 Mahasiswa mampu menunjukkan sikap bijak dan etis dalam praktik social engineering yang banyak merugikan masyarakat	Kriteria: Rubrik holistik Bentuk Penilaian : Aktifitas Partisipasif	Ceramah, diskusi 3 X 50	Ceramah, diskusi 3 x 50	Materi: Metode pencegahan kebocoran data Pustaka: Modul Praktikum Data Security Management	5%
16	Mahasiswa mampu menyikapi penggunaan teknologi informasi dengan bijak, etis, dan efisien untuk mencegah terjadinya kebocoran data	16.1 Mahasiswa mampu menunjukkan sikap bijak dan etis dalam praktik social engineering yang banyak merugikan masyarakat	Kriteria: Rubrik holistik Bentuk Penilaian : Tes	Tes tulis 3 X 50	Tes tulis 3 x 50	Materi: Social engineering Pustaka: Modul Praktikum Data Security Management	30%

Rekap Persentase Evaluasi : Case Study

No	Evaluasi	Persentase
1.	Aktifitas Partisipasif	51%
2.	Praktik / Unjuk Kerja	9%
3.	Tes	40%
		100%

Catatan

- 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.
- 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, ketrampilan umum, ketrampilan khusus dan pengetahuan.
- 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.
- 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.
- 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.
- 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.
- Bentuk penilaian:** tes dan non-tes.
- 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.
- 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.
- 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

Koordinator Program Studi S1
Bisnis Digital



Hujjatullah Fazlurrahman, S.E.,
MBA.
NIDN 0723108603

UPM Program Studi S1 Bisnis
Digital



NIDN

File PDF ini digenerate pada tanggal 8 April 2025 Jam 17:42 menggunakan aplikasi RPS-OBE SiDia Unesa

