<table>
<tr><td rowspan="3"></td><td colspan="2">KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
INSTITUT INFORMATIKA & BISNIS DARMAJAYA
Jl. Zainal Abidin Pagar Alam No. 93 Labuhan Ratu – Bandar Lampung
35142</td><td>No. Dokumen
4.FM-D2.04.03</td></tr>
<tr><td colspan="2">FORMULIR
RENCANA PEMBELAJARAN SEMESTER (RPS)</td><td></td></tr>
<tr><td>No. Revisi
01</td><td>Hal
1 dari
16</td><td>Tanggal Terbit
13 Juni 2021</td></tr>
<tr><td>Matakuliah :
Keamanan Sistem Informasi</td><td>Semester:
5 [Lima]</td><td>Sks :
4 [Empat]</td><td>Kode MK:SIF21427</td></tr>
<tr><td>Program Studi : S1 – Sistem Informasi</td><td colspan="3">Dosen Pengampu/Penanggungjawab : Hendra Kurniawan, S.Kom., M.T.I</td></tr>
<tr><td>Capaian Pembelajaran Lulusan (CPL)</td><td colspan="3"><u>Sikap</u>
1. Mampu menerapkan etika profesi dalam praktik keamanan informasi.
2. Mampu menunjukkan sikap bertanggung jawab dan akuntabel dalam setiap tugas.
3. Mampu menunjukkan sikap disiplin, tepat waktu, dan teliti dalam mengelola keamanan informasi.
4. Mampu menunjukkan inisiatif dan kreativitas dalam memecahkan masalah keamanan informasi.
5. Mampu beradaptasi dengan perubahan dan perkembangan teknologi keamanan informasi.
6. Mampu menerima kritik dan saran dengan sikap terbuka.
7. Mampu menunjukkan rasa peduli terhadap dampak sosial dan etika dari penggunaan teknologi informasi.
8. Mampu memimpin dan berkolaborasi dalam tim keamanan informasi.
9. Mampu berkomunikasi secara efektif dan asertif mengenai isu-isu keamanan informasi.</td></tr>
</table>

	Keterampilan Umum 1. Mampu menjelaskan konsep keamanan informasi kepada audiens non-teknis. 2. Mampu menulis laporan analisis risiko dan rekomendasi keamanan yang komprehensif. 3. Mampu melakukan presentasi tentang topik keamanan informasi dengan jelas dan percaya diri. 4. Mampu mengidentifikasi kerentanan dan ancaman keamanan dalam suatu sistem. 5. Mampu mengevaluasi dan memilih solusi keamanan yang tepat. 6. Mampu bekerja sama dalam tim untuk merespons insiden keamanan. 7. Mampu mencari dan mempelajari informasi terbaru tentang keamanan siber. **CP Keterampilan Khusus** 1. Mampu mengkonfigurasi firewall untuk memblokir akses yang tidak sah. 2. Mampu melakukan enkripsi data menggunakan algoritma kriptografi. 3. Mampu mendeteksi dan merespons serangan malware. 4. Mampu melakukan vulnerability assessment dan penetration testing pada sistem. 5. Mampu membuat laporan analisis keamanan dan rekomendasi perbaikan. 6. Mampu menggunakan tools keamanan seperti Nmap, Wireshark, Metasploit. **Pengetahuan** 1. Mampu menjelaskan konsep dasar keamanan informasi dengan benar. 2. Mampu mengidentifikasi dan menganalisis ancaman dan risiko keamanan informasi. 3. Mampu menjelaskan berbagai jenis serangan dan kejahatan siber. 4. Mampu menjelaskan teknologi dan mekanisme keamanan yang relevan. 5. Mampu menjelaskan standar dan kerangka kerja keamanan informasi. 6. Mampu menjelaskan proses manajemen risiko keamanan informasi. 7. Mampu menjelaskan hukum dan etika terkait keamanan informasi.
Capaian Pembelajaran Matakuliah (CPMK)	1. Memahami secara utuh tentang keamanan sistem baik perngertian, dasar sistem keamanan 2. Memahami dan mampu menerapkan konsep dasar keamanan dalam sistem informasi serta metode dalam penyampaian informasi yaitu Steganografi, Kriptografi, Enkripsi, Kunci Private, kunci public, kombinasi kunci priPvate dan public 3. Memahami berbagai macam tinjauan kemanan pada Sistem Informasi, kemanan komputer, kemanan email, keamanan web, keamanan system wireless berkaitan dengan exploitasi, gangguan serta metode penanggunalangannya 4. Memahami konsep komunikasi sistem dalam pertukaran informasi. 5. Mengerti dan memahami peraturan perundang-undangan yang berkaitan dengan Cyber law serta UU-ITE

Deskripsi Matakuliah	Mata kuliah ini bertujuan memberikan pemahaman tentang pengertian keamanan, pengertian sistem dan pengertian keamanan sistem, evaluasi keamanan sistem, mengamankan sistem informasi, keamanan email, keamanan web, eksploitasi keamanan sistem, enkripsidekripsi, kriptografi, steganografi, firewall, cyber law, dan keamanan sistem nirkabel.

Minggu Ke-	**Kemampuan yang diharapkan (Sub- CPMK)**	**Bahan Kajian/Pokok Bahasan**	**Bentuk, Metode Pembelajaran dan Pengalaman Belajar**	**Waktu (menit)**	**Penilaian**		
					Indikator	**Teknik**	**Bobot**
1	a. Mampu menjelaskan tinjauan sistem kemanan Data b. Mampu menjelaskan pengertian Informasi dan tinjauan dari sistem keamanan c. Mampu menjelaskan pengertian sistem ditinjau dari sistem kemanan d. Mampu menjelaskan pengertian kemanan dalam tinjauan sistem	1.Data 2.Informasi 3. Sistem 4. Keamanan	Ceramah, demonstrasi,tanya-jawab, *small group disscusion*	4x50’	Aspek Kognitif, Aspek Afektif	Penilaian hasil kajian dan diskusi	80% Ranah kognitif 20% Ranah afektif

2	keamanana. Mampu menjelaskan keamanan dan kerahasisaan data dalamsistemkemanan b.Mengerti dan memahami klasifikasi tentang kejahatan komputer c. Memahami aspek dari kemananan d.Memahami proses mendeteksi, mencegah terhadap serangan sistem keamanan e.Mengetahui berbagai macam metoda pengamanan sistem	Klasifikasi kejahatan komputer, Aspek dari Security, Serangan terhadap keamanan Sistem, metode pengamanan sistem	Ceramah, demonstrasi,tanya-jawab, *small group disscusion*	4x50’	Aspek Kognitif, Aspek Afektif	Penilaian hasil kajian dan diskusi	80% Ranah kognitif 20% Ranah afektif
3-5	a.Memahami dasar-dasar kemanan sistem b.Mengetahui jenis- jenis penerapan kemanan sistem steganografi,	Steganografi, Kriptografi, Enkripsi, Kunci Private, kunci public, kombinasi	Ceramah, demonstrasi,tanya-jawab, *small group disscusion*	4x50’	Aspek Kognitif, Aspek Afektif	Penilaian hasil kajian dan diskusi	80% ranah kognitif 20% ranah afektif

	kriptografi, enkripsi, kunci private, kunci public, kombinasi kunci private dan public c. Memahami dan mampu menerapkan konsep steganografi d. Memahami dan mampu menerapkan konsep dasar sistem kemanan Kriptografi e. Memahami dan mampu menerapkan konsep dasar kemanan Enkripsi / Dekripsi f. Memahami dan mampu menerapkan konsep dasar sistem keamanan Kunci private dan Kunci public g. Mampu memahami dan menerapkan	kunci private dan public						

	Konsep dasar keamanan kombinas kunci private dan public						
6-7	a. Mampu memahami dan menjelaskan Tinjauan Evaluasi yang terdapat dalam Keamanan Sistem Informasi b. Mampu memahami dan menjeaskan Evaluasi Sistem Keamanan sistem Informasi tentang Lubang Keamanan c. Mampu melakukan pengujian keamanan sistem dalam Evaluasi Keamanan sistem Informasi d. Mampu melakukan probing services dalam keamanan sistem informasi e. Mampu menggunakan	Sumber lubang keamanan, Penguji keamanan sistem, Probing services, Penggunaan program penyerang, penggunaan program pemantau jaringan.	Ceramah, demonstrasi,tanya-jawab, *small group disscusion*	4x50’	Aspek Kognitif, Aspek Afektif	Penilaian hasil kajian dan diskusi	80% ranah kognitif 20% ranah afektif

	program penyerangan dan program pemantau jaringan dalam melakukan uji coba sistem keamanan Sistem Informasi						
8	a. Memahami konsep keamanan komputer b. Mengetahui dan mampu menjelaskan siklus hidup pengembangan sistem	Keamanan komputer, Lifecycle pengembangan Sistem	Ceramah, demonstrasi,tanya-jawab, *small group disscusion*	4x50’	Aspek Kognitif, Aspek Afektif	Penilaian hasil kajian dan diskusi	80% ranah Kognitif 20% ranah afektif
9-10	a. Mampu memahami dan melakukan bagaimana proses dalam mengamankan Sistem b. Mampu memahami dan melakukan pengaturan hak akses c. Mengetahui berbagai macam	Mengatur akses, menutup service yang tidak digunakan, memasang proteksi (*Firewall*), Pemantau adanya serangan, audit, backup rutin.	Ceramah, demonstrasi,tanya-jawab, *small group disscusion*	4x50’	Aspek Kognitif, Aspek Afektif	Penilaian hasil kajian dan diskusi	80% ranah kognitif 20% ranah afektif

	service serta penggunaannya d. Memahami firewall dan mampu menggunakan dalam proses pengamanan						
11	a. Mampu memahami dan melakukan pengamanan terhadap email b. Mengetahui konsep format email ditinjau dalam sistem kemanan c. Mengetahui dan mampu Menjelaskan bagaimana proses penyadapan penyusupan virus dan pemalsuan email. Memahami dan menjelaskan mail bomb dan mail relaying	Format email, penyadapan, pemalsuan, penyusupan virus, mail bomb, mail relaying.	Ceramah, demonstrasi,tanya-jawab, *small group disscusion*	4x50’	Aspek Kognitif, Aspek Afektif	Penilaian hasil kajian dan diskusi	80% ranah kognitif 20% ranah afektif
12	a. Mengetahui, memahami dan menerapkan	Keamanan web, keamanan	Ceramah, demonstrasi,tanya-jawab, *small*	4x50’	Aspek Kognitif, Aspek Afektif	Penilaian hasil kajian dan diskusi	80% ranah kognitif 20% ranah afektif

	kemanan web b. Memahami dan menjelaskan kemanann client dalamsuatu web	client www,	*group disscusion* i				
13	a. Memahami dan mampu menjelaskan konsep komunikasi yang digunakan dalam sebuah system b. Memahami cara sistem jaringan berkomunikasi c. Memahami komunikasi router d. Memahami anatomi frame data e. Memahami dan mampu menjelaskan berbagai macam protocol yang terdapat dalam jaringan a. Memahami	Anatomi frame data, Protokol, Router	Ceramah, demonstrasi,tanya-jawab, *small group disscusion*	4x50’	Aspek Kognitif, Aspek Afektif	Penilaian hasil kajian dan diskusi	80% ranah kognitif 20% ranah afektif
14	konsep kemanan dalam sistem Komunikasi berbasis wireless	Wireless, WiFi, Mobile phone, Keamanan Wi Fi	Ceramah, demonstrasi,tanya-jawab, *small group disscusion*	4x50’	Aspek Kognitif, Aspek Afektif	Penilaian hasil kajian dan diskusi	80% ranah kognitif 20% ranah afektif

	b.Memahami berbagai macam komunikasi menggunakan wireless c. Memahami konsep pengiriman dalam komunikasi wireless						
15	a. Mampumen jelaskan Berbagai macam Eksploitasi yang biasa dilakukan dalam sistem keamanan b. Memahami konsep dan berbagai informasi tentang webserver c. Memahami konsep dan cara DDOS, Sniffer dan Trojan horse bekerja	Mencari informasi, eksploitasi webserver, DDOS, Sniffer, Trojan horse.	Ceramah, demonstrasi,tanya-jawab, *small group disscusion*	4x50’	Aspek Kognitif, Aspek Afektif	Penilaian hasil kajian dan diskusi	80% ranah kognitif 20% ranah afektif
16	a. Memahami aturan perundangan mengenai Cyberlaw	Cyberlaw, UU ITE	Ceramah,tanya-jawab, *small group disscusion*	4x50’	Aspek Kognitif, Aspek Afektif	Penilaian hasil kajian dan diskusi	80% ranah kognitif 20% ranah afektif

Referensi:
1.Budi Raharjo, 2005. KeamananSistemInformasi, PT InsanInfonesia , Jakarta

Bandar Lampung, 13 Juni 2021

Disusun oleh	Diperiksa oleh	Diperiksa oleh	Disahkan oleh
Hendra Kurniawan, M.T.I **Dosen Penanggungjawab**	**Penanggungjawab Kelompok Bidang Keilmuan (KBK)**	**Ketua Program Studi Sistem Informasi**	**Dekan** **Fakultas Ilmu Komputer**